8 10/100TX plus 2 100/1000TX/Mini-GBIC combo Managed Industrial Switch

User Manual

HMG-828

Rev.2.0

05-Mar-2007

Notice

This manual contents are based on the below table listing software kernel version, hardware version, and firmware version. If the switch functions have any different from the manual contents description, please contact the local sale dealer for more information.

Firmware Version	V1.09
Kernel Version	V2.01
Hardware Version	----------

FCC Warning

This Equipment has been tested and found to comply with the limits for a Class-A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

CE Mark Warning

This is a Class-A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Content

FCC Warning 1

CE Mark Warning..... 1

Introduction..... 1

Features..... 1

Package Contents..... 2

Hardware Description 3

Physical Dimension..... 3

Front Panel 3

Bottom View..... 4

LED Indicators 5

Ports..... 7

Cabling..... 8

Wiring the Power Inputs..... 10

Wiring the Fault Alarm Contact..... 10

Wiring the Fault Alarm Contact..... 11

Mounting Installation 12

DIN-Rail Mounting..... 12

Wall Mount Plate Mounting 14

Hardware Installation 15

Installation Steps..... 15

Network Application..... 16

X-Ring Application 16

Coupling Ring Application..... 17

Dual Homing Application..... 18

Web-Based Management..... 19

About Web-based Management 19

Preparing for Web Management..... 19

System Login 20

System Information 21

IP Configuration 21

DHCP Server – System configuration..... 22

DHCP Client – System Configuration 23

DHCP Server - Port and IP Bindings 24

TFTP - Update Firmware 24

TFTP – Restore Configuration 25

TFTP - Backup Configuration 25

System Event Log – Syslog Configuration..... 26

System Event Log - SMTP Configuration 27
System Event Log - Event Configuration 28
Fault Relay Alarm 30
SNTP Configuration 31
IP Security 33
User Authentication 34
Port Statistics 35
Port Control 35
Port Trunk 36
Aggregator setting 37
Aggregator Information 38
State Activity 38
Port Mirroring 39
Rate Limiting 40
VLAN configuration 41
VLAN configuration - Port-based VLAN 42
802.1Q VLAN 45
802.1Q Configuration 46
Group Configuration 46
Rapid Spanning Tree 48
RSTP System Configuration 48

RSTP Per Port Configuration 49
SNMP Configuration 50
System Configuration 50
Trap Configuration 51
SNMPV3 Configuration 52
QoS Configuration 56
QoS Policy and Priority Type 56
Port Base Priority 57
COS Configuration 58
TOS Configuration 58
IGMP Configuration 58
X-Ring 60
802.1X/Radius Configuration 61
System Configuration 62
802.1x Per Port Configuration 63
Misc. Configuration 63
MAC Address Table 64
Static MAC Address 64
MAC Filtering 65
All MAC Addresses 66
Factory Default 67
Save Configuration 67
System Reboot 68

Troubleshooting 68

Technical Specifications..... 70

Introduction

The 8 10/100TX plus 2 Gigabit Copper/Mini GBIC managed industrial switch is a cost-effective solution and meets the high reliability requirements demanded by industrial applications. The 8 10/100TX plus 2 Gigabit Copper/Mini GBIC managed industrial switch can be easily managed through the Web GUI. By using fiber port can extend the connection distance that increases the network elasticity and performance. It also provides the X-Ring function that can prevent the network connection failure.

Features

- Conforms to IEEE 802.3 10Base-T, 802.3u 100Base-TX, 1000Base-TX
- 8-port 10/100TX plus 2 1000TX/Mini-GBIB combo port industrial switch
- RJ-45 port supports auto MDI/MDI-X function
- Store-and-Forward switching architecture
- Wide-range redundant power inputs
- DIN rail and wall mount
- Easy configuration
- 8K MAC address table
- Web management GUI
- Supports 4 priority queues per port
- Provides Fiber link capability
- IEEE 802.3x flow control support
  - Flow control with full-duplex
  - Back pressure with half-duplex
- Supports Class of service (CoS)
- Supports IGMP with Query mode for multi media application
- Supports ingress packet filter and egress rate limit.
- Supports SNTP/SMTP
- Port mirroring for TX or RX or TX and RX packets.
- Alarm Relay output for system events

- Supports X-Ring function (Ring Redundancy)
- Reverse Power polarity protection
- 1Mbits Embedded memory
- Supports Port based VLAN / 802.1 Q Tag VLAN
- Quality of Service: (QoS)
  - Supports IEEE 802.1p class of service
  - Provides 4 priority queues per port
  - Port based/Tag based, IPv4 ToS, IPv4 Different Service
- Support DHCP client
- SNMP, Web Management, RMON support
- TFTP firmware update and system configuration - restore and backup.

Package Contents

Please refer to the package content list below to verify them against the checklist.

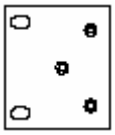
- 8 10/100TX plus 2 1000TX/Mini-GBIB combo managed industrial switch
- User manual
- RS-232/RJ-45 cable
- Block connector
- One DIN-Rail (attached on the switch)
- 2 wall mount plates and 6 screws

8 10/100TX plus 2 1000LX/SX managed industrial switch

User Manual

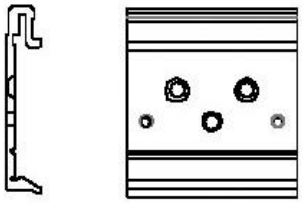
RS-232/RJ-45 connector cable

block connector



Wall Mount Plate

Screws



DIN-Rail

Compare the contents of the industrial switch with the standard checklist above. If any item is damaged or missing, please contact the local dealer for service.

Hardware Description

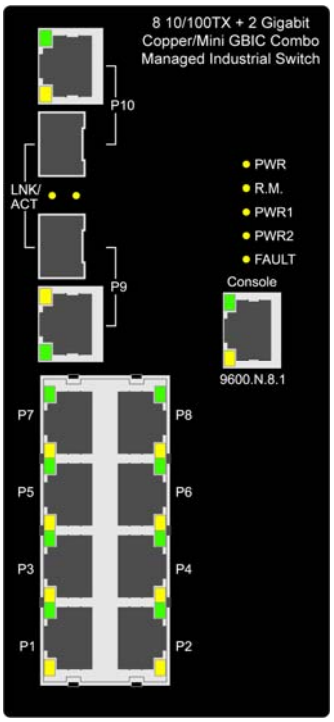
In this section, we will describe the Industrial switch's hardware spec, port, cabling information, and wiring installation.

Physical Dimension

8 10/100TX plus 2 1000TX/Mini-GBIB combo managed industrial switch dimension (W x D x H) is **72mm x 105mm x 152mm**

Front Panel

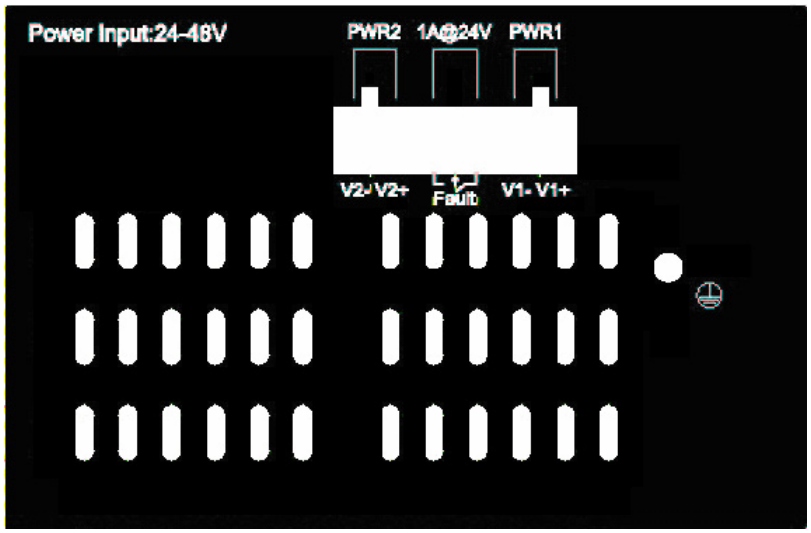
The Front Panel of the 8 10/100TX plus 2 100FX managed industrial switch is shown as below:



Front Panel of the industrial switch

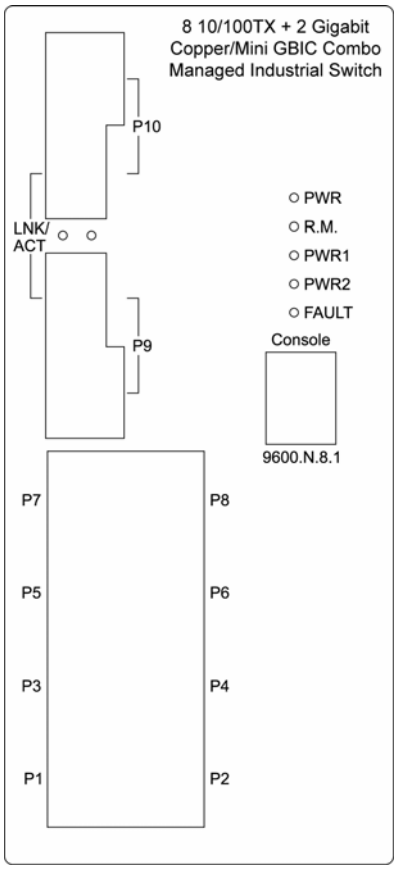
Bottom View

The bottom panel of the 8 10/100TX plus 2 1000LX/SX managed industrial switch has one terminal block connector within two DC power inputs and one DC IN power jack.



Bottom Panel of the industrial switch

LED Indicators



LED indicators

There are 7 diagnostic LEDs located on the front panel of the industrial switch. They provide real-time information of system and optional status. The following table provides description of the LED status and their meanings for the switch.

LED	Status	Meaning
PWR	Green	The switch unit is power on
	Off	The switch unit is no power input
PWR1	Green	Power on
	Off	No power inputs
PWR2	Green	Power on

	Off	No power inputs
Fault	Orange	Power failure or UTP port failure or Fiber port failure
	Off	No Power failure or UTP port failure or Fiber port failure occurs
R.M.	Green	The industrial switch is the master of X-Ring group
	Off	The industrial switch is not a ring master in X-Ring group
LNK/ACT	Green	The fiber port is linking
	Blinks	The port is transmitting or receiving packets from the TX device.
	Off	No device attached
P1 ~ P8	Orange	The port is operating in full-duplex mode.
	Blinking (Orange)	Collision of Packets occurs.
	Off	The port is in half-duplex mode or no device is attached.
	Green	A network device is detected.
	Blinking (Green)	The port is transmitting or receiving packets from the TX device.
	Off	No device attached

Ports

- **RJ-45 ports**

There are 8x 10/100Mbps auto-sensing ports for 10Base-T or 100Base-TX devices connection. The UTP ports will auto-sense for 10Base-T or 100Base-TX connections. Auto MDI/MDIX means that the switch can connect to another switch or workstation without changing straight through or crossover cabling. See the below figures for straight through and crossover cable schematic.

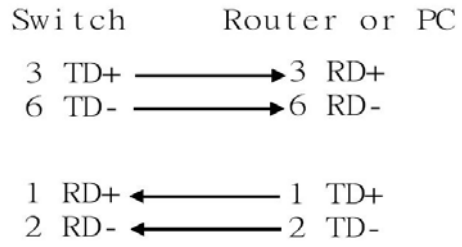
- **RJ-45 Pin Assignments**

Pin Number	Assignment
1	Tx+
2	Tx-
3	Rx+
6	Rx-

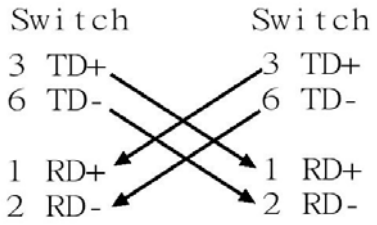
[NOTE] "+" and "-" signs represent the polarity of the wires that make up each wire pair.

All ports on this industrial switch support automatic MDI/MDI-X operation, the user can use straight-through cables (See figure below) for all network connections to PCs or servers, or to other switches or hubs. In straight-through cable, pins 1, 2, 3, and 6, at one end of the cable, are connected straight through to pins 1, 2, 3 and 6 at the other end of the cable. The table below shows the 10BASE-T/100BASE-TX MDI and MDI-X port pin outs.

Pin MDI-X	Signal Name	MDI Signal Name
1	Receive Data plus (RD+)	Transmit Data plus (TD+)
2	Receive Data minus (RD-)	Transmit Data minus (TD-)
3	Transmit Data plus (TD+)	Receive Data plus (RD+)
6	Transmit Data minus (TD-)	Receive Data minus (RD-)



Straight Through Cable Schematic



Cross Over Cable Schematic

2 Mini GBIC/Giga copper combo port: 2 auto-detect Giga port—UTP or fiber. Giga fiber is the mini GBIC module that is optional.. These two ports are 1000BASE-T copper ports (provided) and Mini-GBIC ports (optional). See the diagram below to view the two Mini-GBIC port modules being plugged into the Switch. Please note that although these two front panel modules can be used simultaneously, the ports must be different. The GBIC port will always have the highest priority.

■

ATTENTION

This is a Class 1 Laser/LED product. Don't stare into the Laser/LED Beam.

Cabling

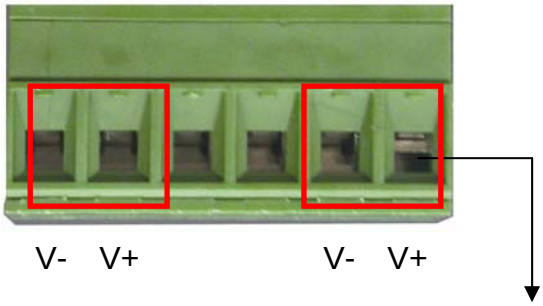
■ Using four twisted-pair, Category 5 cabling for a RJ-45 port connection. The cable

between the converter and the link partner (switch, hub, workstation, etc.) must be less than 100 meters (328 ft.) long.

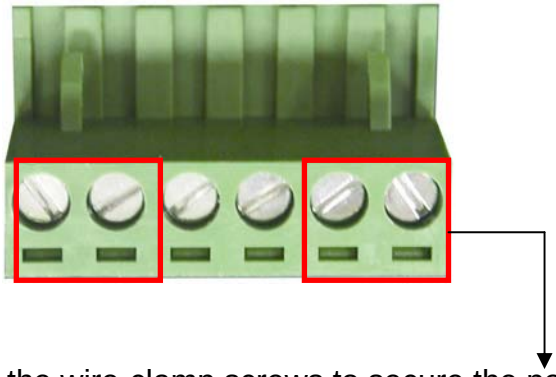
- Fiber segment using **single-mode** connector type must use 8/125 or 9/125 um single-mode fiber cable. User can connect two devices in the distance up to **30 Kilometers**.
- Fiber segment using **multi-mode** connector type must use 50 or 62.5/125 um multi-mode fiber cable. User can connect two devices up to **2Km** distances.

Wiring the Power Inputs

Please follow the below steps to insert the power wire.



1. Insert the positive and negative wires into the V+ and V- contacts on the terminal block connector.

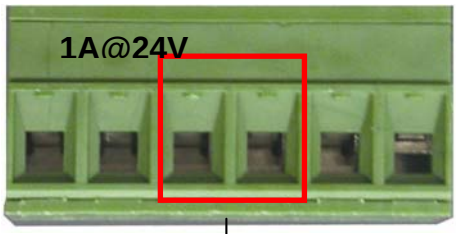


2. Tighten the wire-clamp screws to secure the power wiring.

[NOTE] The wire range of terminal block is from 12~ 24 AWG.

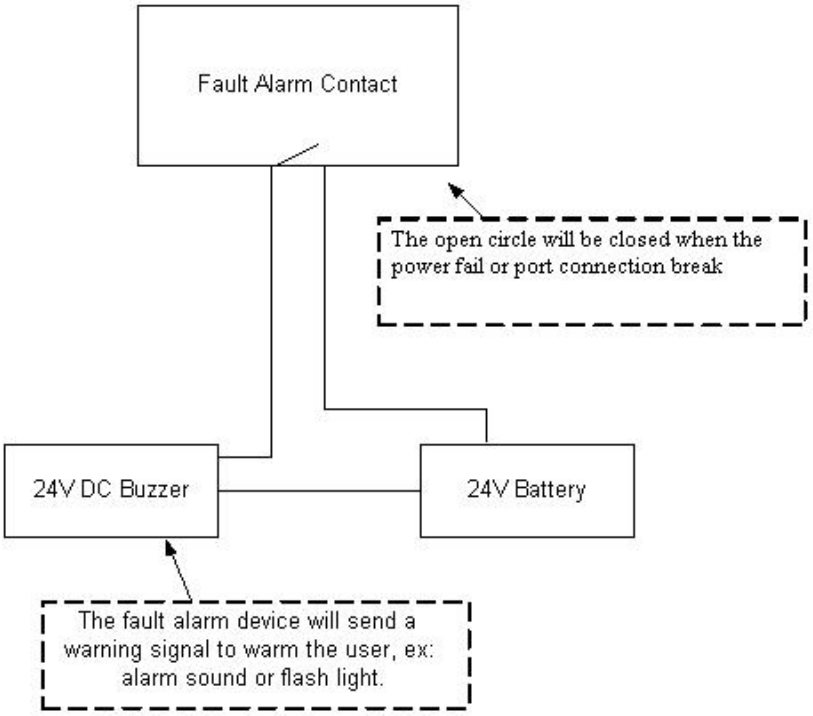
Wiring the Fault Alarm Contact

The fault alarm contact is in the middle of terminal block connector as below picture shows. By inserting the wires, it will detect the fault status for power failure or port link failure and form an open circuit. And, application example for the fault alarm contact as below:



Insert the wires into the fault alarm contact

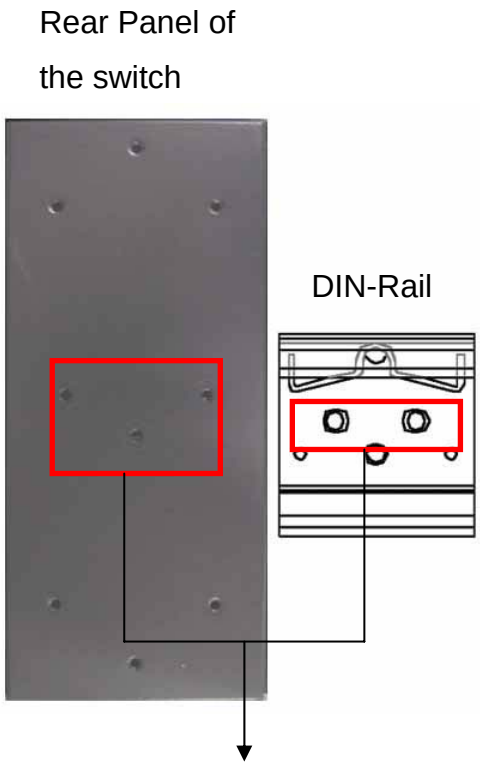
[NOTE] The wire range of terminal block is from 12~ 24 AWG.


Fault Alarm Contact
The open circle will be closed when the power fail or port connection break
24V DC Buzzer
24V Battery
The fault alarm device will send a warning signal to warm the user, ex: alarm sound or flash light.

Mounting Installation

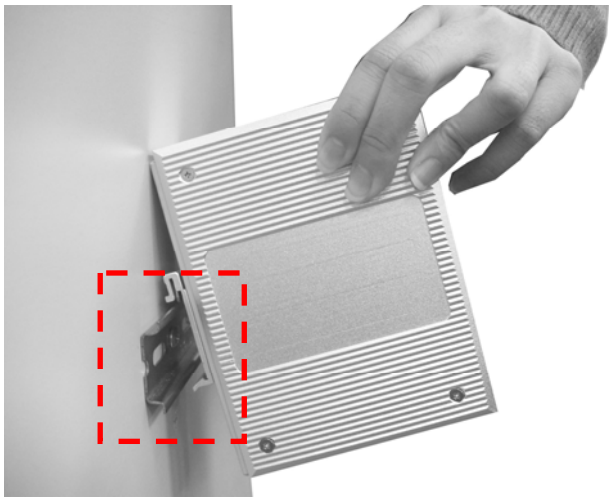
DIN-Rail Mounting

The DIN-Rail is screwed on the industrial switch from the factory. If the DIN-Rail is not screwed on the industrial switch, please see the following pictures to screw the DIN-Rail on the switch. Follow the below steps to mount the DIN Rail mount to the industrial switch.

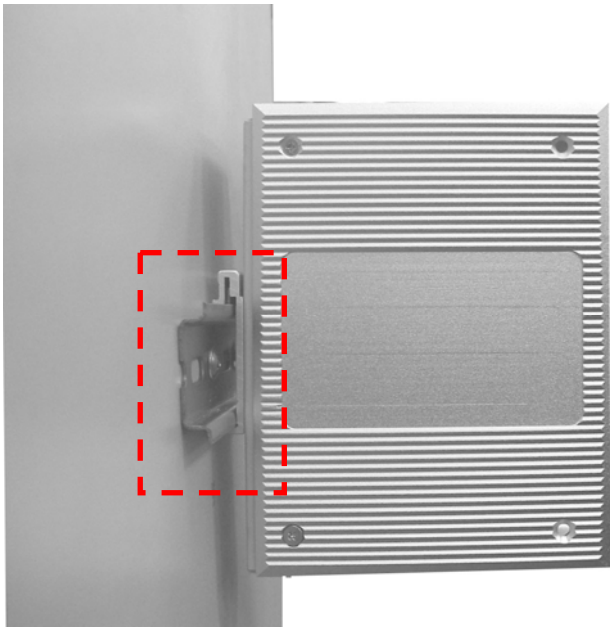


1. Use the screws to screw the DIN-Rail on the industrial switch
2. To remove the DIN-Rail, reverse the step 1.

1. First, insert the top of DIN-Rail into the track.



2. Then, lightly push the DIN-Rail into the track.

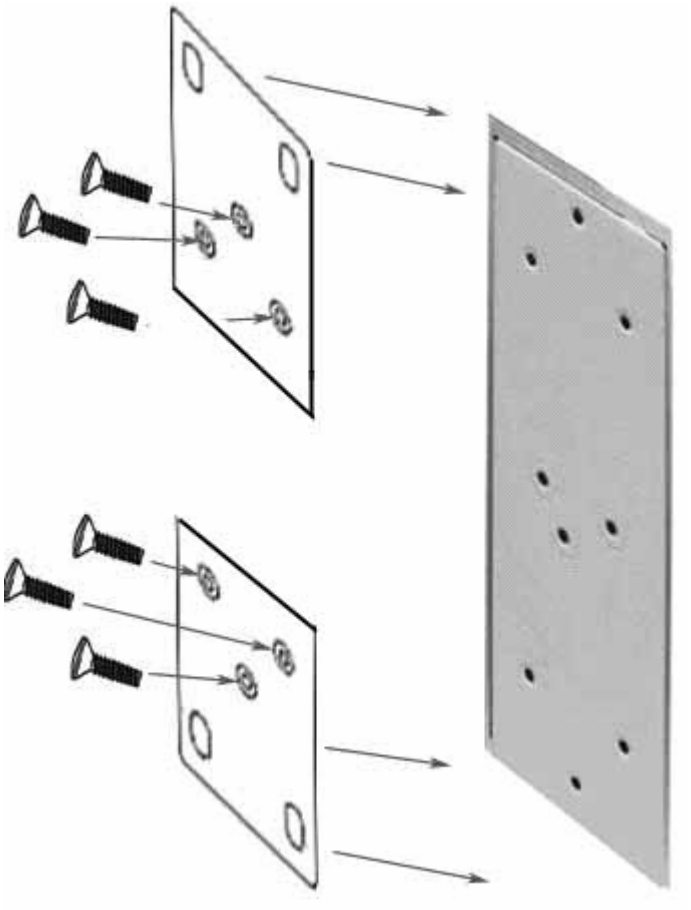


3. Check if the DIN-Rail is tightened on the track.
4. To remove the industrial switch from the track, reverse the steps above.

Wall Mount Plate Mounting

Follow the below steps to mount the industrial switch with the wall mount plate.

1. Remove the DIN-Rail from the industrial switch; loosen the screws to remove the DIN-Rail.
2. Place the wall mount plate on the rear panel of the industrial switch.
3. Use the screws to screw the wall mount plate on the industrial switch.
4. Use the hook holes at the corners of the wall mount plate to install the industrial switch on the wall.
5. To remove the wall mount plate, reverse steps above.



Screwing the wall mount plate on the Industrial switch.

Hardware Installation

In this section, we will describe how to install the 8 10/100TX plus 2 1000LX/SX Managed Industrial Switch.

Installation Steps

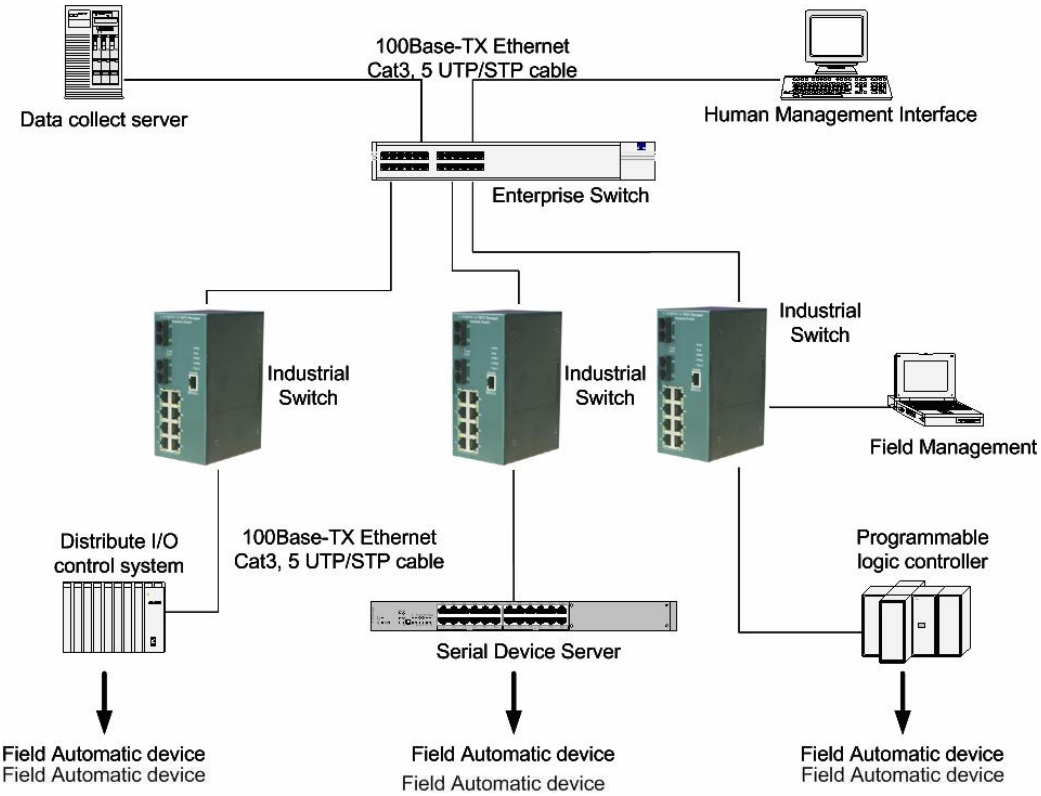
1. Unpack the Industrial switch
2. Check if the DIN-Rail is screwed on the Industrial switch or not. If the DIN-Rail is not screwed on the Industrial switch, please refer to **DIN-Rail Mounting** section for DIN-Rail installation. If the user wants to wall mount the Industrial switch, then please refer to **Wall Mount Plate Mounting** section for wall mount plate installation.
3. To mount the Industrial switch on the DIN-Rail track or wall, please refer to the **Mounting Installation** section.
4. Apply power to the Industrial switch. Please refer to the **Wiring the Power Inputs** section for the information about how to wire the power inputs. The power LED on the Industrial switch will light up. Please refer to the **LED Indicators** section for indication of LED lights.
5. Prepare the twisted-pair, straight through Category 5 cable for Ethernet connection.
6. Insert one side of RJ-45 cable (category 5) into the Industrial switch Ethernet port (RJ-45 port) and another side of RJ-45 cable (category 5) to the network device's Ethernet port (RJ-45 port), ex: Switch PC or Server. The UTP port (RJ-45) LED on the Industrial switch will light up when the cable is connected with the network device. Please refer to the **LED Indicators** section for LED light indication.

   [NOTE] Make sure that the connected network devices support MDI/MDI-X. If it does not support, then use the crossover category-5 cable.

7. When all connections are set and LED lights all show in normal, the installation is complete.

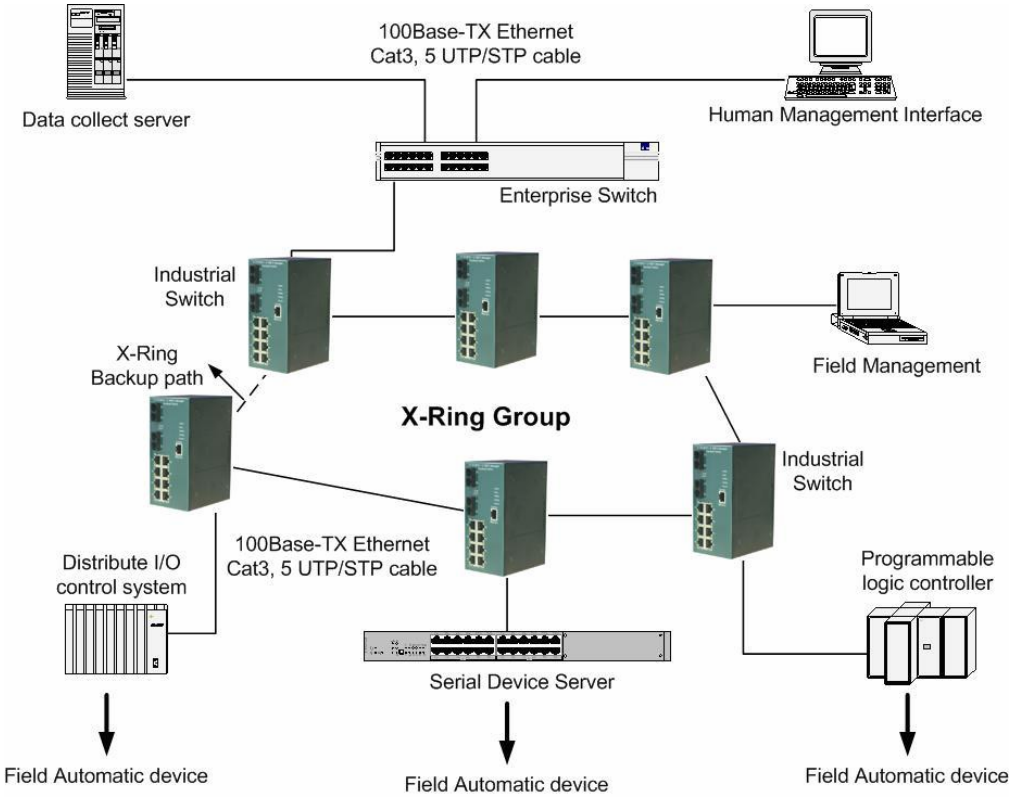
Network Application

This chapter provides some sample applications to help user to have more actual idea of industrial switch function application. A sample application of the industrial switch is as below:



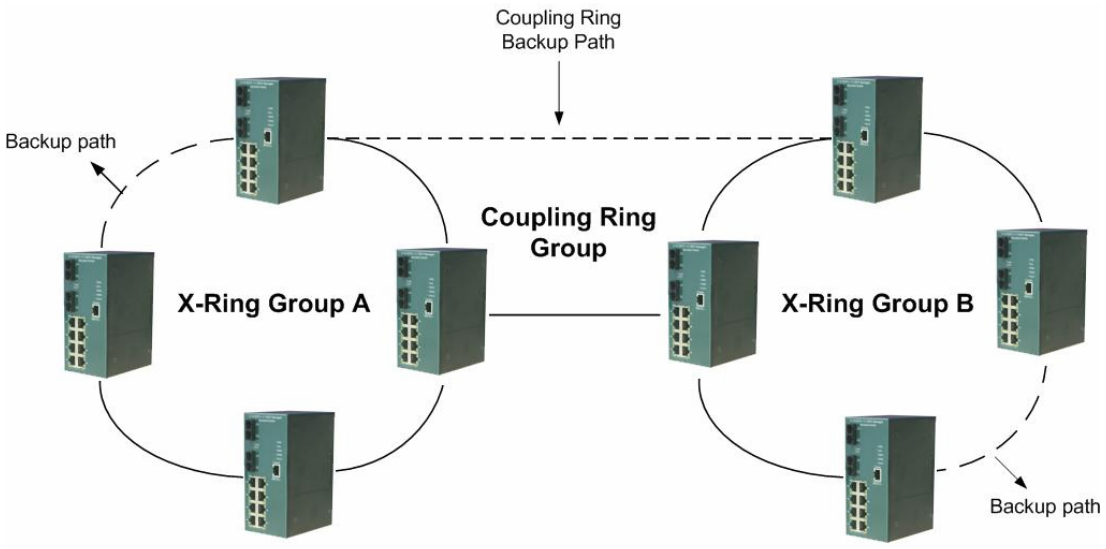
X-Ring Application

The industrial switch supports the X-Ring protocol that can help the network system to recovery from network connection failure within 300ms or less, and make the network system more reliable. The X-Ring algorithm is similar to spanning tree protocol (STP) algorithm but its recovery time is faster than STP. The following figure is a sample X-Ring application.



Coupling Ring Application

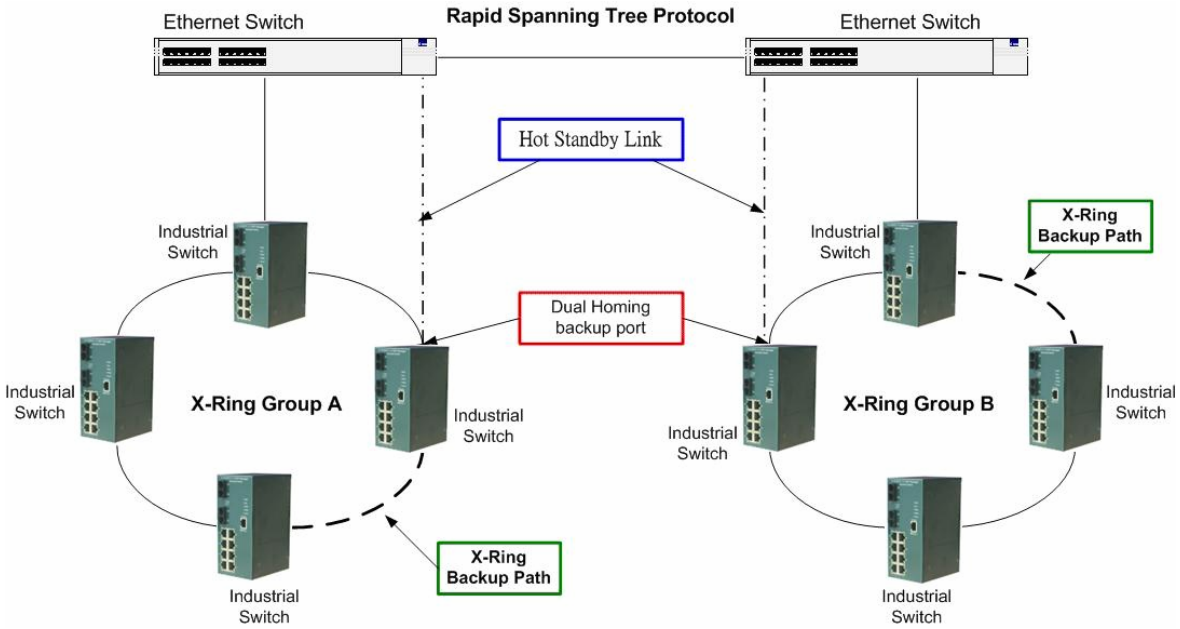
A network may have more than one X-Ring. By using the coupling ring function, it can connect each X-Ring to the redundant backup. It can ensure the transmissions between two ring groups will not fail. The following figure is a sample of coupling ring application.



Dual Homing Application

Dual Homing function is to prevent connection loss from between an X-Ring group and upper level/core switches. Assign two ports to be the Dual Homing port that is the backup port in the X-Ring group. The Dual Homing function only works when the X-Ring function is active. Each X-Ring group has only one Dual Homing port.

[NOTE] In a Dual Homing application architecture, the upper level switches need to enable the Rapid Spanning Tree protocol.



Web-Based Management

This section introduces the configuration and functions of the Web-Based management.

About Web-based Management

On the CPU board of the switch there is an embedded HTML web site residing in flash memory, which offers advanced management features and allow users to manage the switch from anywhere on the network through a standard browser such as Microsoft Internet Explorer.

The Web-Based Management supports Internet Explorer 5.0. And, it is applied for Java Applets for reducing network bandwidth consumption, enhance access speed and present an easy viewing screen.

[NOTE] By default, IE5.0 or later versions do not allow Java Applets to activate sockets. The user has to explicitly modify the browser setting to enable Java Applets to operate network ports.

Preparing for Web Management

Before using web management, install the industrial switch on the network and make sure that one of the PCs on the network can connect with the industrial switch through the web browser. The industrial switch default value of IP, subnet mask, username and password is as below:

- IP Address: **192.168.16.1**
- Subnet Mask: **255.255.255.0**
- Default Gateway: **192.168.16.254**

- User Name: **root**
- Password: **root**

System Login

1. Launch the Internet Explorer on the PC
2. Key in “http:// “+” the IP address of the switch”, and then Press “**Enter**”.

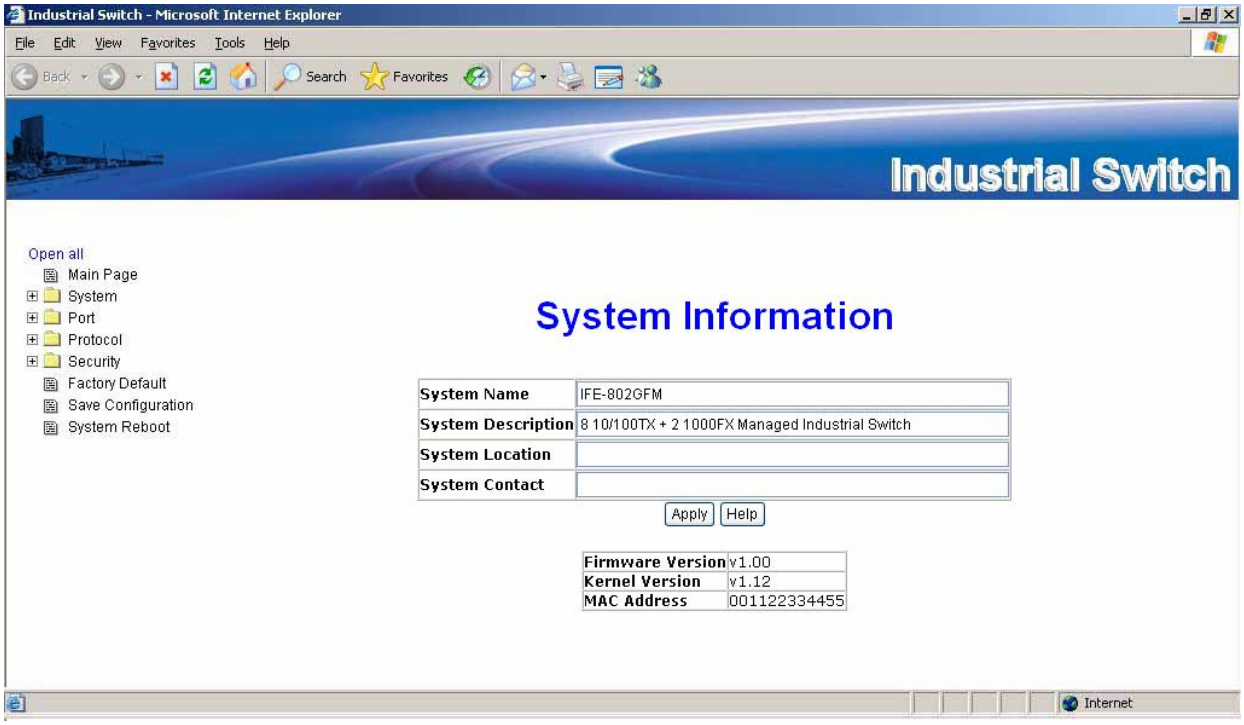
3. The login screen will appear right after
4. Key in the user name and password. The default user name and password are the same as “**root**”
5. Press “**Enter**” or ”**OK**”, and then the home screen of the Web-based management appears as below:

Login screen

System Information

Assigning the system name, location and view the system information

- **System Name:** Assign the name of switch. The maximum length is 64 bytes
- **System Description:** Display the description of switch. Read only cannot be modified
- **System Location:** Assign the switch physical location. The maximum length is 64 bytes
- **System Contact:** Enter the name of contact person or organization
- **Firmware Version:** Display the switch's firmware version
- **Kernel Version:** Display the kernel software version
- **MAC Address:** Display the unique hardware address assigned by manufacturer (default)



Switch settings interface

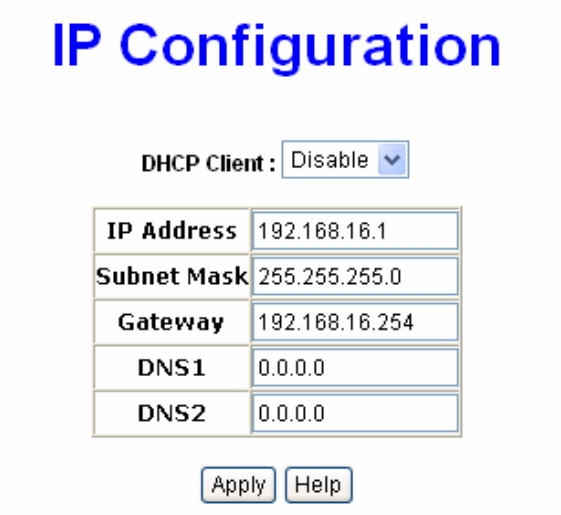
IP Configuration

The User can configure the IP Settings and DHCP client function

- **DHCP Client:** To enable or disable the DHCP client function. When the DHCP client function is enabled, the industrial switch will be assigned the IP address from

the network DHCP server. The default IP address will be replaced by the DHCP server assigned IP address. After the user clicks the “Apply” button, a popup dialog is shown. It is to inform the user that when the DHCP client is enabled, the current IP will be lost and user should find the new IP on the DHCP server. To cancel enabling DHCP client function, click “cancel”

- **IP Address:** Assign the IP address that the network is using. If DHCP client function is enabled, and the user doesn’t need to assign the IP address. The network DHCP server will assign the IP address for the industrial switch and display in this column. The default IP is 192.168.16.1
- **Subnet Mask:** Assign the subnet mask of the IP address. If DHCP client function is enabling, and then user does not need to assign the subnet mask
- **Gateway:** Assign the network gateway for the industrial switch. The default gateway is 192.168.16.254
- **DNS1:** Assign the primary DNS IP address
- **DNS2:** Assign the secondary DNS IP address
- And then, click Apply



IP configuration interface

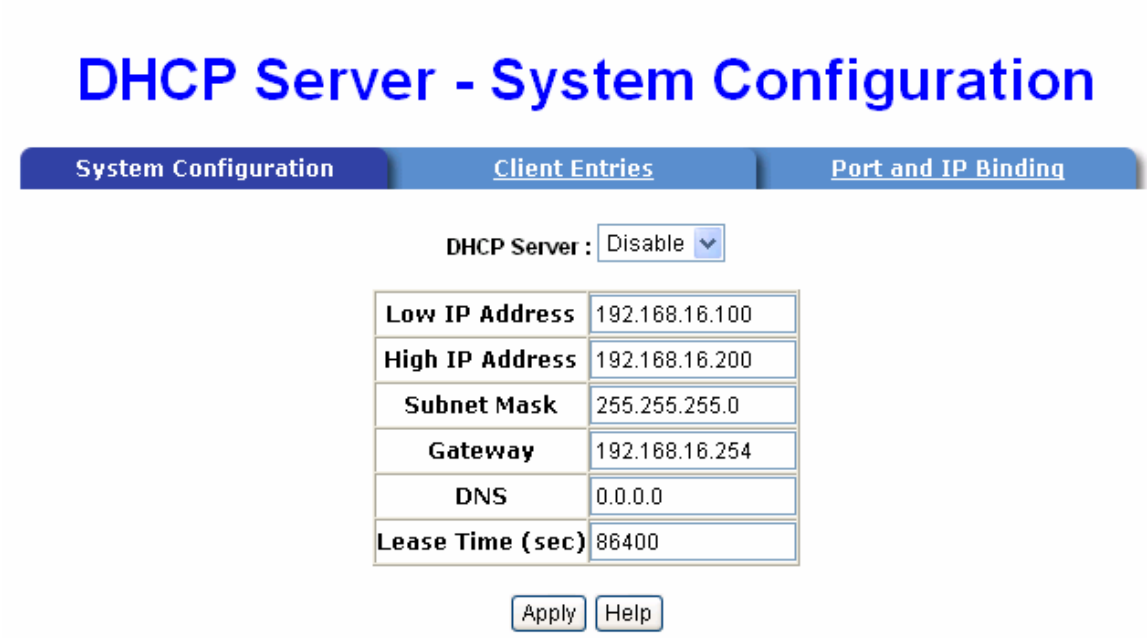
DHCP Server – System configuration

The system provides the DHCP server function. Enabling the DHCP server function and the switch will be assigned address information by a DHCP server.

- **DHCP Server:** Enable or Disable the DHCP Server function. Enable – the switch

will be the DHCP server on your local network.

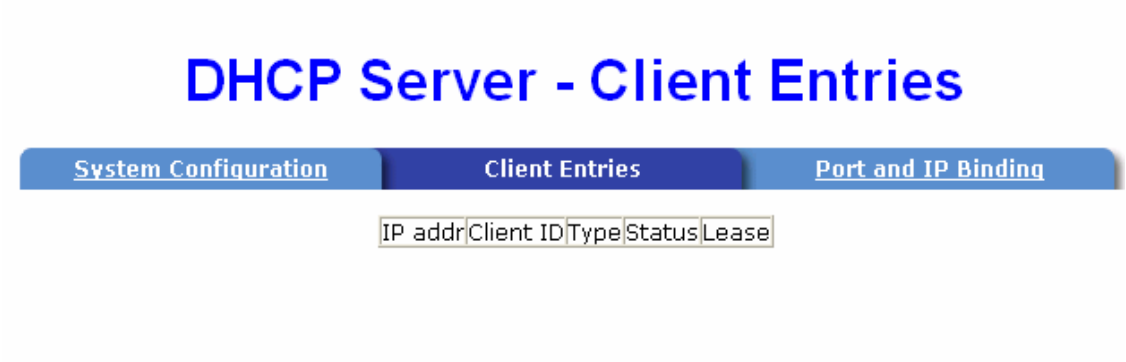
- **Low IP Address:** the dynamic IP assign range. The Low IP address is the beginning of the dynamic IP assigns range. For example: dynamic IP assign range is from 192.168.1.100 ~ 192.168.1.200. 192.168.1.100 will be the Low IP address.
- **High IP Address:** the dynamic IP assign range. The High IP address is the end of the dynamic IP assigns range. For example: dynamic IP assign range is from 192.168.1.100 ~ 192.168.1.200. 192.168.1.200 will be the High IP address.
- **Subnet Mask:** the dynamic IP assign range subnet mask.
- **Gateway:** the gateway in your network.
- **DNS:** Domain Name Server IP Address in your network.
- **Lease Time (sec):** It is the time period that system will reset the dynamic IP assignment to ensure the dynamic IP will not been occupied for a long time or the server doesn't know that the dynamic IP is idle.
- And then, click Apply



DHCP Server Configuration interface

DHCP Client – System Configuration

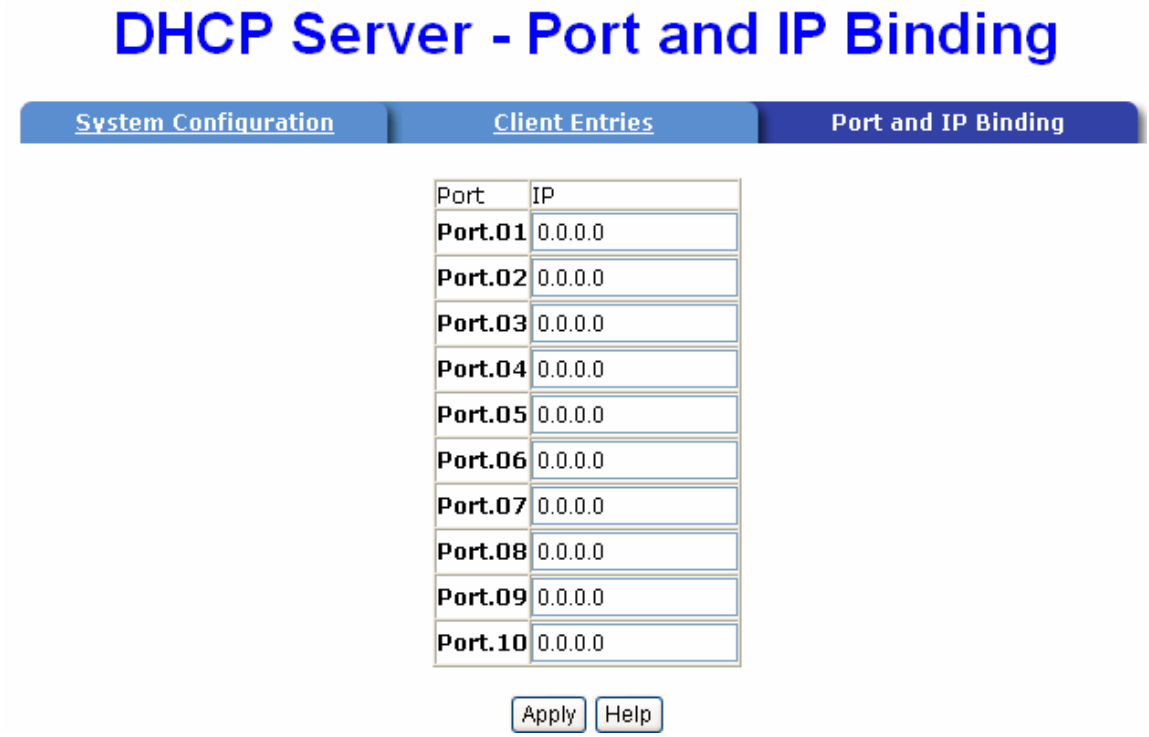
When the DHCP server function is active, the system will collect the DHCP client information and display it here.



DHCP Client Entries interface

DHCP Server - Port and IP Bindings

You can assign the specific IP address that is the IP in dynamic IP assign range to the specific port. When the device is connecting to the port and asks for dynamic IP assigning, the system will assign the IP address that has been assigned before to the connected device.



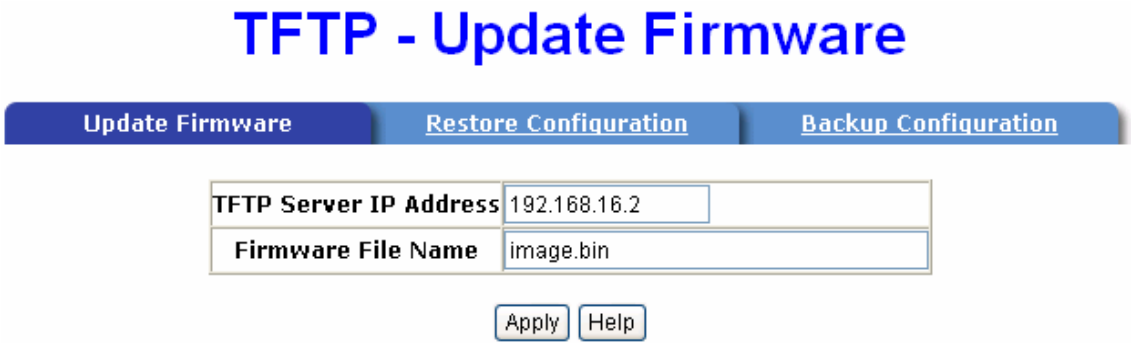
Port and IP Bindings interface

TFTP - Update Firmware

It provides the functions to allow a user to update the switch firmware. Before updating, make sure you have your TFTP server ready and the firmware image is on the TFTP server.

1. **TFTP Server IP Address:** fill in your TFTP server IP.

2. **Firmware File Name:** the name of firmware image.
3. Click Apply.

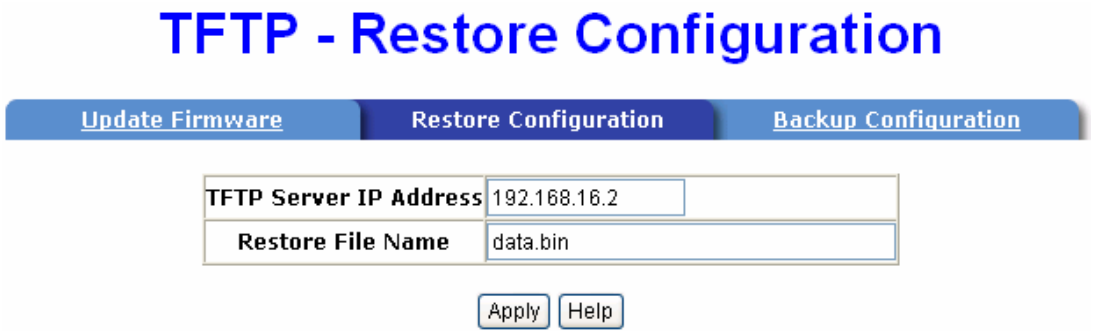


Update Firmware interface

TFTP – Restore Configuration

You can restore the EEPROM value from the TFTP server, but you must put back the image in TFTP server, switch will download the flash image.

1. **TFTP Server IP Address:** fill in the TFTP server IP.
2. **Restore File Name:** fill in the correct restore file name.
3. Click Apply.

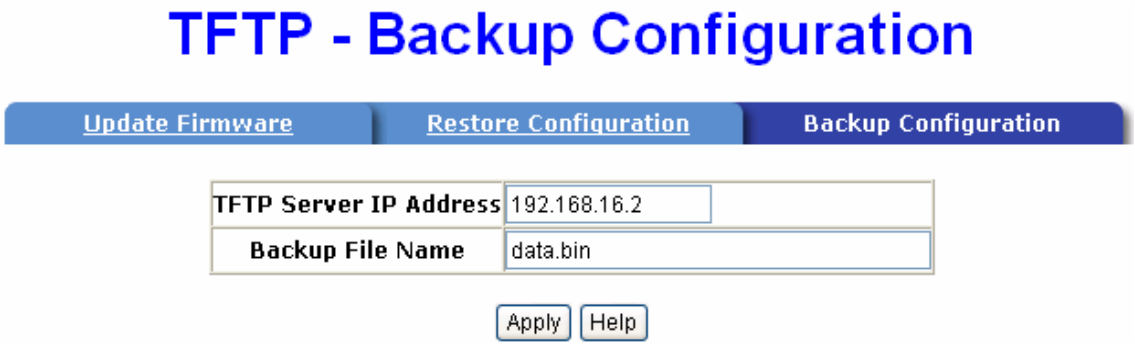


Restore Configuration interface

TFTP - Backup Configuration

You can save current EEPROM value from the switch to the TFTP server, then go to the TFTP to restore the configuration page in the EEPROM memory.

1. **TFTP Server IP Address:** fill in the TFTP server IP
2. **Backup File Name:** fill the file name
3. Click Apply.

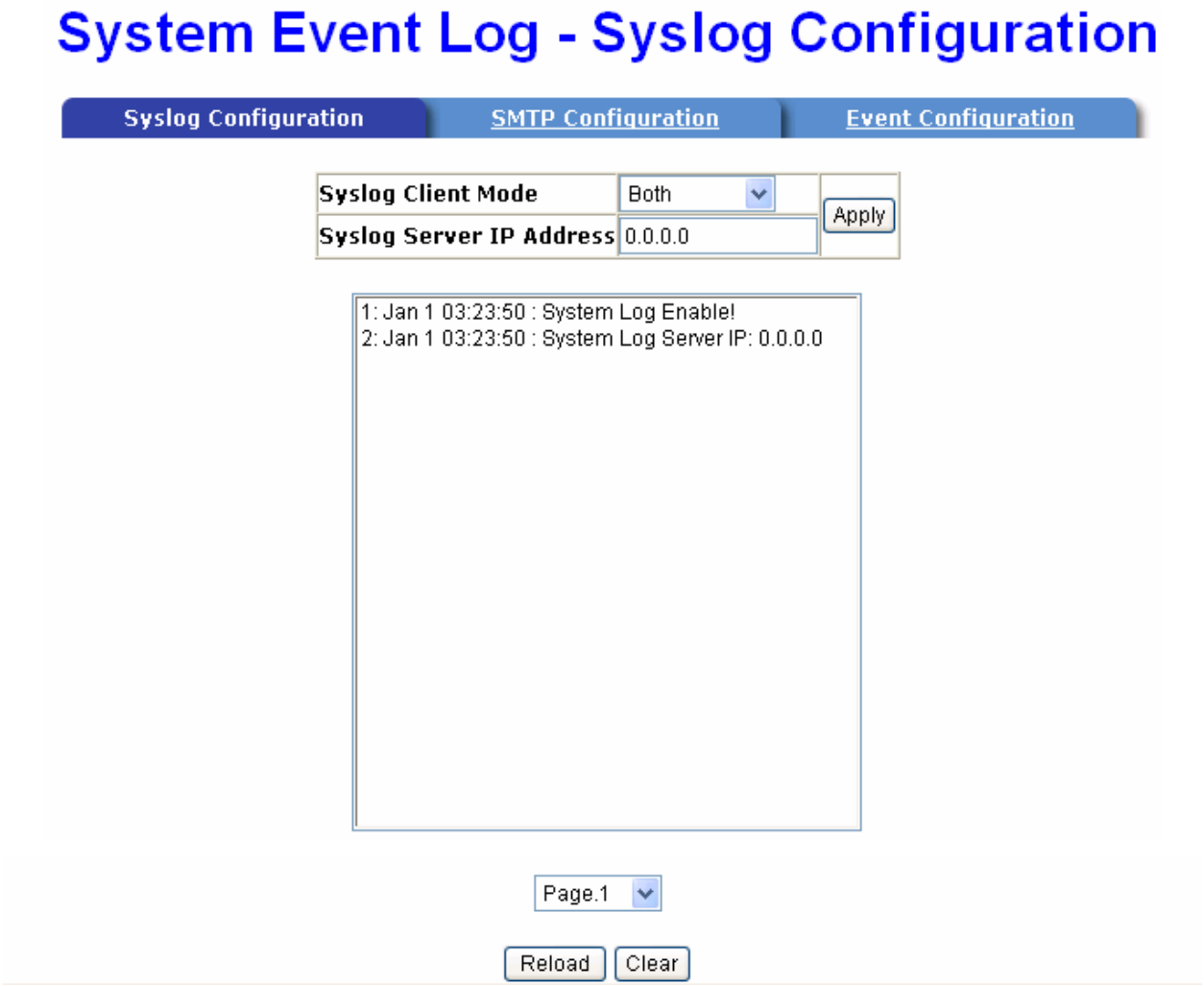


Backup Configuration interface

System Event Log – Syslog Configuration

Configuring the system event mode that want to be collected and system log server IP.

1. **Syslog Client Mode:** select the system log mode – client only, server only, or both S/C.
2. **System Log Server IP Address:** assigned the system log server IP.
3. Click Reload to refresh the events log.
4. Click Clear to clear all current events log.
5. After configuring, Click Apply.



Syslog Configuration interface

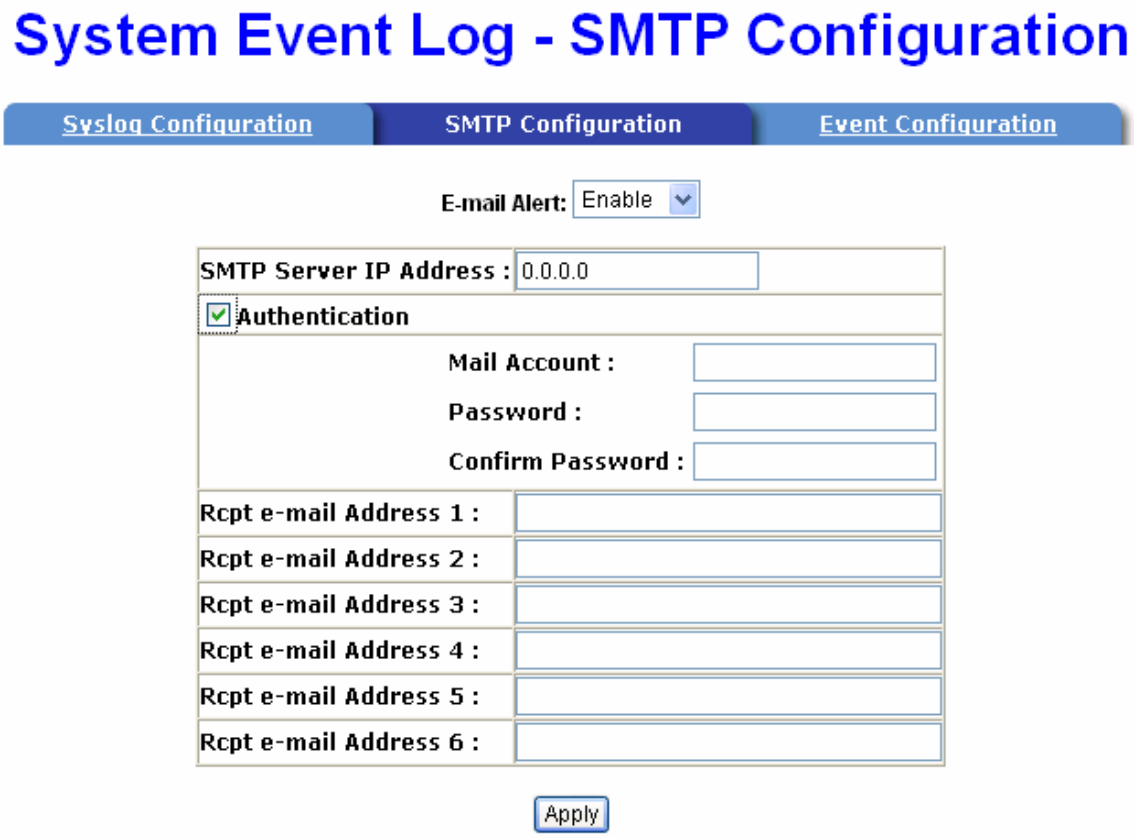
System Event Log - SMTP Configuration

You can set up the mail server IP, mail account, account password, and forwarded email account for receiving the event alert.

1. **Email Alert:** enable or disable the email alert function.
2. **SMTP Server IP:** set up the mail server IP address (when **Email Alert** enabled, this function will then be available)..
3. **Authentication:** mark the check box to enable and configure the email account and password for authentication (when **Email Alert** enabled, this function will then be available)..
4. **Mail Account:** set up the email account to receive the alert. Ex: johnadmin@123.com. It must be an existing email account on the mail server,

which you had set up in **SMTP Server IP Address** column.

5. **Password:** The email account password.
6. **Confirm Password:** reconfirm the password.
7. **Rcpt e-mail Address 1 ~ 6:** you can assign up to 6 e-mail accounts also to receive the alert.
8. Click Apply.



SMTP Configuration interface

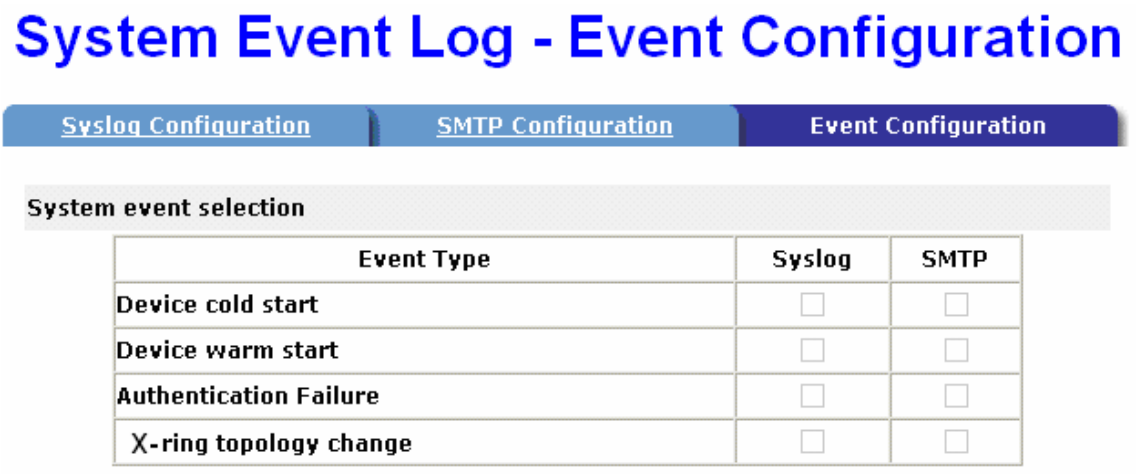
System Event Log - Event Configuration

You can select the system log events and SMTP events. When selected events occur, the system will send out the log information. Also, per port log and SMTP events can be selected. After configure, Click Apply.

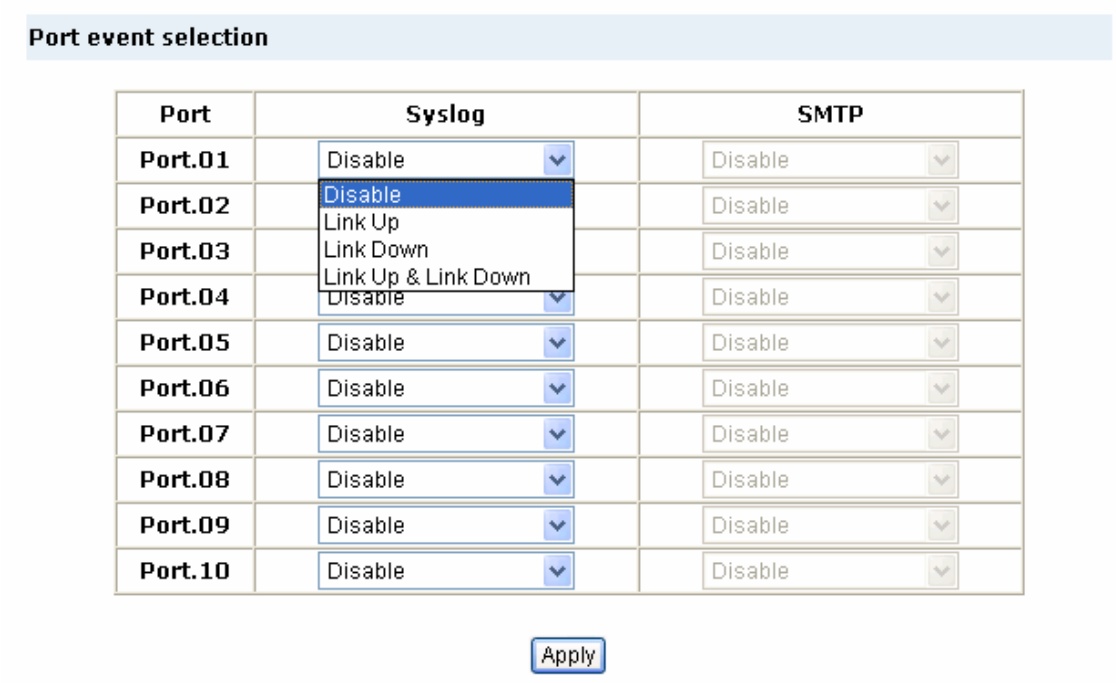
- **System event selection:** 4 selections – Device cold start, Device warm start,

SNMP Authentication Failure, and X-ring topology change. Mark the checkbox to select the event. When selected events occur, the system will issue the logs.

- **Device cold start:** when the device executes a cold start action, the system will issue a log event.
- **Device warm start:** when the device executes **a** warm start, the system will issue a log event.
- **Authentication Failure:** when the SNMP authentication fails, the system will issue a log event.
- **X-ring topology change:** when the X-ring topology has changed, the system will issue a log event.



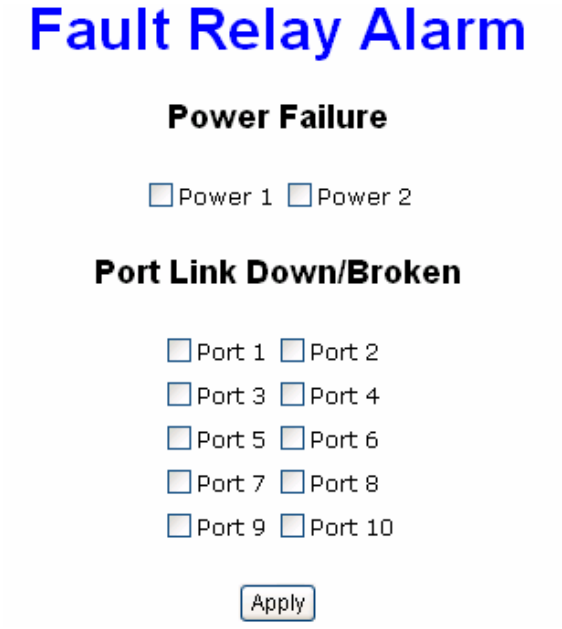
- **Port event selection:** select the per port events and per port SMTP events. It has 3 selections – Link UP, Link Down, and Link UP & Link Down. Disable means no event is selected.
  - **Link UP:** the system will issue a log message when port connection is up.
  - **Link Down:** the system will issue a log message when port connection is down.
  - **Link UP & Link Down:** the system will issue a log message when port connection is up and down.



Event Configuration interface

Fault Relay Alarm

- **Power Failure:** Mark the check box to enable the function of lighting up the **FAULT** LED on the panel when power fails.
- **Port Link Down/Broken:** Mark the check box to enable the function of lighting up **FAULT** LED on the panel when Ports' states are link down or broken.



Fault Relay Alarm interface

SNTP Configuration

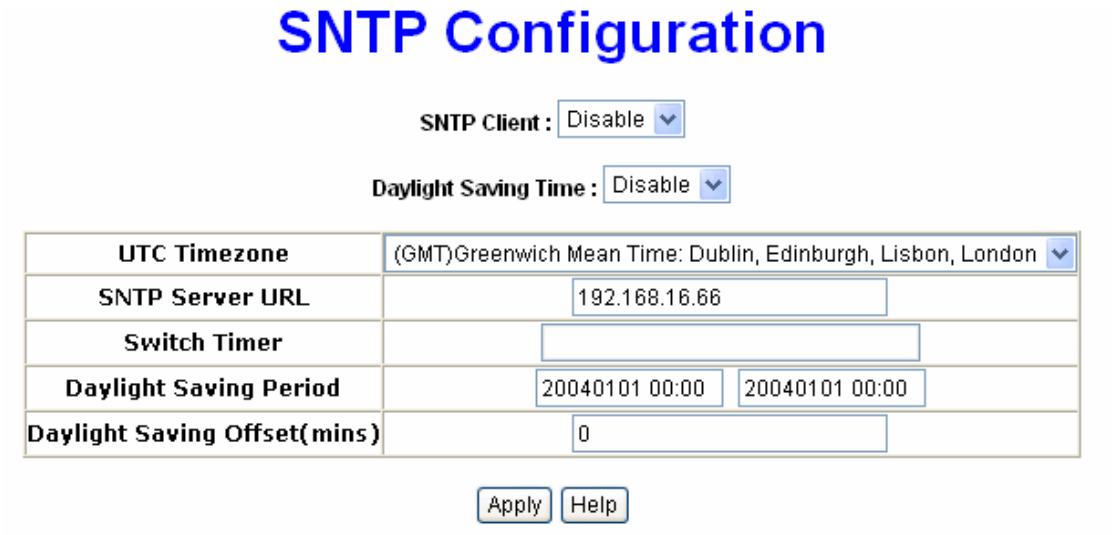
You can configure the SNTP (Simple Network Time Protocol) settings. The SNTP allows you to synchronize switch clocks in the Internet.

1. **SNTP Client:** enable or disable SNTP function to get the time from the SNTP server.
2. **Daylight Saving Time:** enable or disable daylight saving time function. When daylight saving time is enabling, you need to configure the daylight saving time period..
3. **UTC Timezone:** set the switch location time zone. The following table lists the different location time zone for your reference.

Local Time Zone	Conversion from UTC	Time at 12:00 UTC
November Time Zone	- 1 hour	11am
Oscar Time Zone	-2 hours	10 am
ADT - Atlantic Daylight	-3 hours	9 am
AST - Atlantic Standard EDT - Eastern Daylight	-4 hours	8 am
EST - Eastern Standard CDT - Central Daylight	-5 hours	7 am
CST - Central Standard MDT - Mountain Daylight	-6 hours	6 am
MST - Mountain Standard PDT - Pacific Daylight	-7 hours	5 am
PST - Pacific Standard ADT - Alaskan Daylight	-8 hours	4 am
ALA - Alaskan Standard	-9 hours	3 am
HAW - Hawaiian	-10 hours	2 am

Standard		
Nome, Alaska	-11 hours	1 am
CET - Central European FWT - French Winter MET - Middle European MEWT - Middle European Winter SWT - Swedish Winter	+1 hour	1 pm
EET - Eastern European, USSR Zone 1	+2 hours	2 pm
BT - Baghdad, USSR Zone 2	+3 hours	3 pm
ZP4 - USSR Zone 3	+4 hours	4 pm
ZP5 - USSR Zone 4	+5 hours	5 pm
ZP6 - USSR Zone 5	+6 hours	6 pm
WAST - West Australian Standard	+7 hours	7 pm
CCT - China Coast, USSR Zone 7	+8 hours	8 pm
JST - Japan Standard, USSR Zone 8	+9 hours	9 pm
EAST - East Australian Standard GST Guam Standard, USSR Zone 9	+10 hours	10 pm
IDLE - International Date Line NZST - New Zealand Standard NZT - New Zealand	+12 hours	Midnight

4. **SNTP Sever URL:** set the SNTP server IP address.
5. **Daylight Saving Period:** set up the Daylight Saving beginning time and Daylight Saving ending time. Both will be different in every year.
6. **Daylight Saving Offset (mins):** set up the offset time.
7. **Switch Timer:** display the switch current time.
8. Click Apply.



SNTP Configuration interface

IP Security

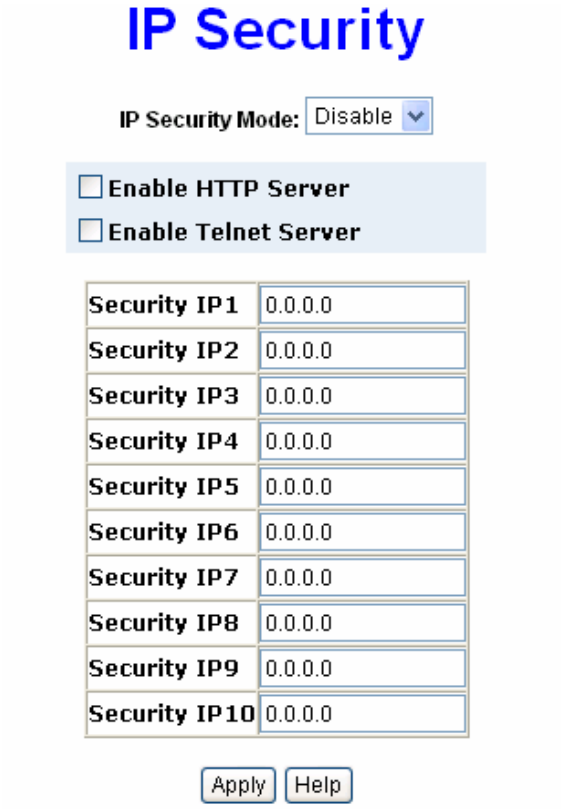
The IP security function allows the user to assign 10 specific IP addresses that have permission to access the switch through the web browser for switch management.

- **IP Security Mode:** when this option is in the **Enable** mode, the **Enable HTTP Server** and **Enable Telnet Server** check boxes will then be available.
- **Enable HTTP Server:** when this check box is checked, the IP addresses among Security IP1 ~ IP10 will be allowed to access via HTTP service.
- **Enable Telnet Server:** when checked, the IP addresses among Security IP1 ~ IP10 will be allowed to access via telnet service.
- **Security IP 1 ~ 10:** Assign up to 10 specific IP address. Only these 10 IP address

can access and manage the switch through the Web browser

- And then, click Apply button to apply the configuration

[NOTE] Remember to execute the “Save Configuration” action, otherwise the new configuration will be lost when switch is powered off.



IP Security interface

User Authentication

Change web management login user name and password for the management security.

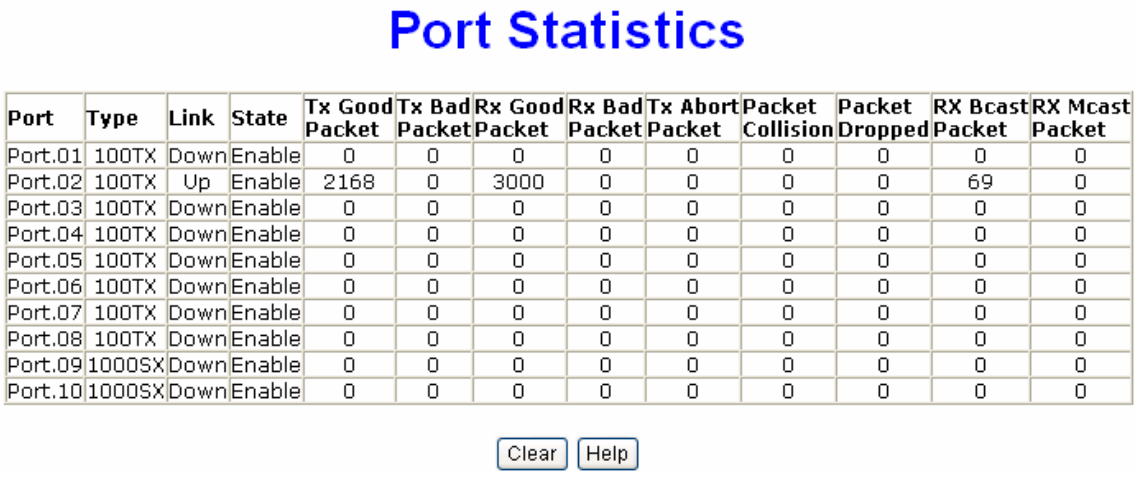
1. **User name:** Key in the new user name(The default is “root”)
2. **Password:** Key in the new password(The default is “root”)
3. **Confirm password:** Re-type the new password
4. And then, click Apply

User Authentication interface

Port Statistics

The following information provides the current port statistic information

- Click Clear button to resets all counts


Port Statistics
Port Type Link State Tx Good Packet Tx Bad Packet Rx Good Packet Rx Bad Packet Tx Abort Packet Packet Collision Packet Dropped RX Bcast Packet RX Mcast Packet
Port.01 100TX Down Enable 0 0 0 0 0 0 0 0 0
Port.02 100TX Up Enable 2168 0 3000 0 0 0 0 69 0
Port.03 100TX Down Enable 0 0 0 0 0 0 0 0 0
Port.04 100TX Down Enable 0 0 0 0 0 0 0 0 0
Port.05 100TX Down Enable 0 0 0 0 0 0 0 0 0
Port.06 100TX Down Enable 0 0 0 0 0 0 0 0 0
Port.07 100TX Down Enable 0 0 0 0 0 0 0 0 0
Port.08 100TX Down Enable 0 0 0 0 0 0 0 0 0
Port.09 1000SX Down Enable 0 0 0 0 0 0 0 0 0
Port.10 1000SX Down Enable 0 0 0 0 0 0 0 0 0
Clear
Help

Port Statistics interface

Port Control

Port control, allows the user to configure the port – speed, Half or Full duplex, Flow control, and negotiation settings.

1. **Port:** select the port that you want to configure.
2. **State:** Current port status. The port can be set to the disable or enable mode. If the port setting is disabled then will not receive or transmit any packets.

3. **Negotiation:** set auto negotiation status of port.
4. **Speed:** set the port link speed.
5. **Duplex:** set full-duplex or half-duplex mode of the port.
6. **Flow Control:** set flow control function is **Symmetric** or **Asymmetric** in Full Duplex mode. The default value is **Disable**.
7. **Security:** When its state is "**On**", means this port accepts only one MAC address.
8. Click Apply.

Port	Group ID	Type	Link	State	Negotiation	Speed Duplex		Flow Control		Security
						Config	Actual	Config	Actual	
Port.01	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Disable	N/A	OFF
Port.02	N/A	100TX	Up	Enable	Auto	100 Full	100 Full	Disable	OFF	OFF
Port.03	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Disable	N/A	OFF
Port.04	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Disable	N/A	OFF
Port.05	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Disable	N/A	OFF
Port.06	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Disable	N/A	OFF
Port.07	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Disable	N/A	OFF
Port.08	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Disable	N/A	OFF
Port.09	N/A	1000SX	Down	Enable	Force	1G Full	N/A	Disable	N/A	OFF
Port.10	N/A	1000SX	Down	Enable	Force	1G Full	N/A	Disable	N/A	OFF

Port Control interface

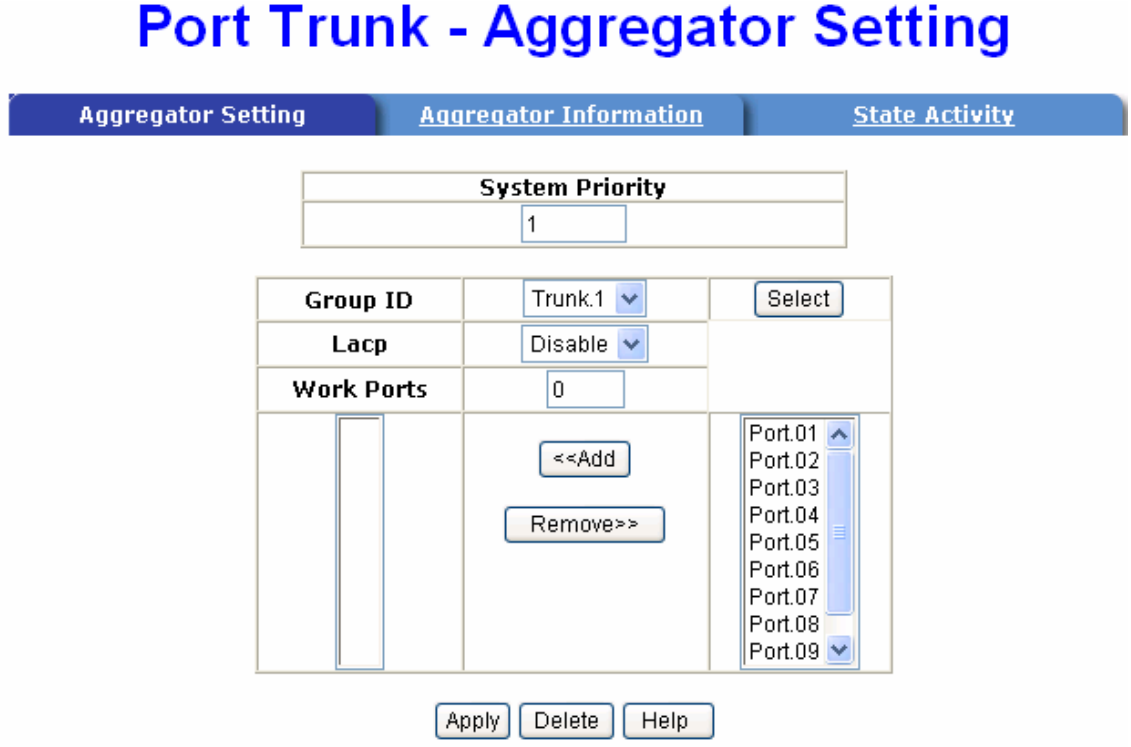
Port Trunk

The Link Aggregation Control Protocol (LACP) provides a standardized means for exchanging information between Partner Systems on a link to allow their Link Aggregation Control instances to reach agreement on the identity of the Link Aggregation Group to which the link belongs, move the link to that Link Aggregation Group, and enable its transmission and reception functions in an orderly manner. Link aggregation lets you group up to seven consecutive ports into two dedicated

connections. This feature can expand bandwidth to a device on the network. **LACP operation requires full-duplex mode,** more detail information refers to IEEE 802.3ad.

Aggregator setting

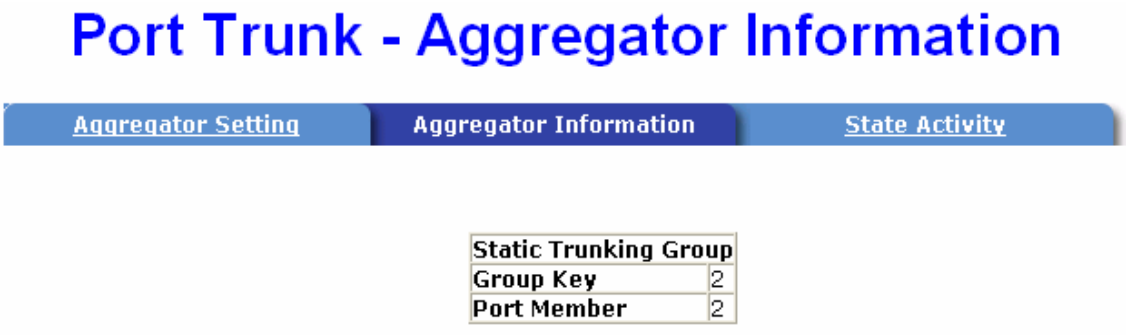
1. **System Priority:** a value used to identify the active LACP. The switch with the lowest value has the highest priority and is selected as the active LACP.
2. **Group ID:** There are three trunk groups to provide configure. Choose the "**Group ID**" and click Select.
3. **LACP:** If enable, the group is LACP static trunk group. If disable, the group is local static trunk group. All ports support LACP dynamic trunk group. If connecting to the device that also supports LACP, the LACP dynamic trunk group will be created automatically.
4. **Work ports:** allow max four ports can be aggregated at the same time. With LACP static trunk group, the exceed ports are standby and can be aggregated if work ports fail. If it is local static trunk group, the number of ports must be the same as the group member ports.
5. Select the ports to join the trunk group. Allow max four ports can be aggregated at the same time. Click Add button to add the port. To remove unwanted ports, select the port and click Remove button.
6. If LACP enable, you can configure LACP Active/Passive status in each ports on State Activity page.
7. Click Apply.
8. Use Delete button to delete Trunk Group. Select the Group ID and click Delete button.



Port Trunk—Aggregator Setting interface

Aggregator Information

When you had setup the LACP aggregator, you will see relation information in here.



Port Trunk – Aggregator Information interface

State Activity

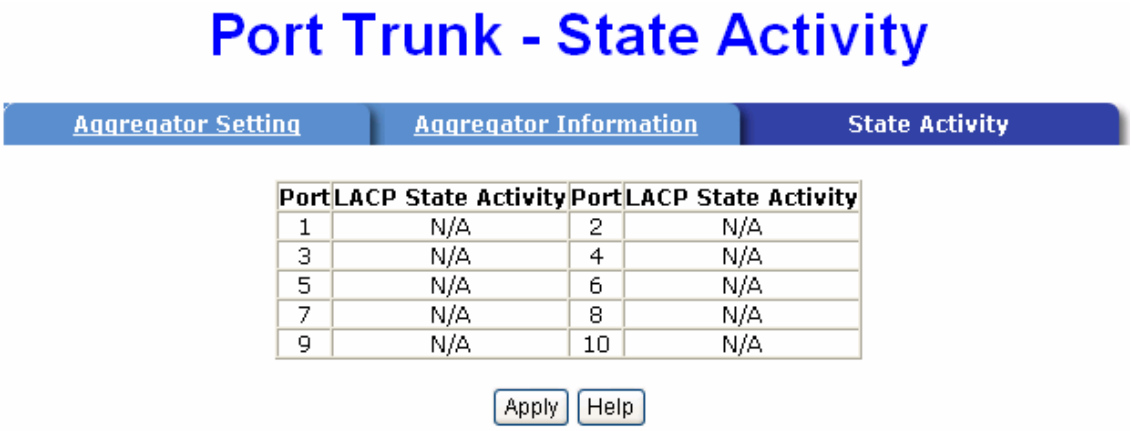
When you had setup the LACP aggregator, you can configure port state activity. You

can mark or un-mark the port. When you mark the port and click Apply button the port state activity will change to **Active**. Opposite is **Passive**.

- **Active:** The port automatically sends LACP protocol packets.
- **Passive:** The port does not automatically send LACP protocol packets, and responds only if it receives LACP protocol packets from the opposite device.

[NOTE]

1. A link having either two active LACP ports or one active port can perform dynamic LACP trunking.
2. A link that has two passive LACP ports will not perform dynamic LACP trunk ing because both ports are waiting for the LACP protocol packet from the opposite device.
3. If you are the active LACP's actor, after you have selected the trunk port, the active status will be created automatically.



Port Trunk – State Activity interface

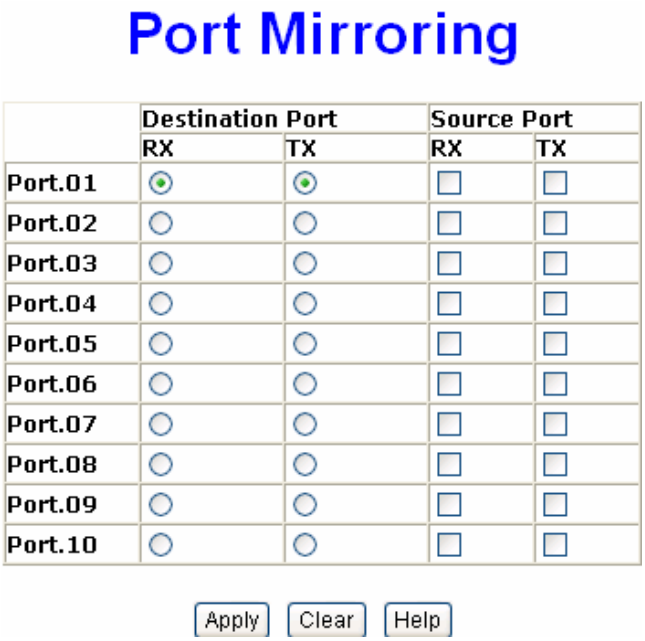
Port Mirroring

The Port mirroring is a method for monitor traffic in switched networks. Traffic through ports can be monitored by one specific port. That means traffic goes in or out monitored (source) ports will be duplicated into the mirrored (destination) port.

- **Destination Port:** There is only one port can be selected to be the destination

(mirror) port for monitoring both RX and TX traffic which comes from the source port. Or, use one of two ports for monitoring RX traffic only and the other one for TX traffic only. The user can connect a mirrored port to a LAN analyzer.

- **Source Port:** The ports that the user wants to monitor. All monitored port traffic will be copied to the mirror (destination) port. The user can select multiple source ports to be monitored by checking the **RX** or **TX** check boxes.
- And then, click Apply button.

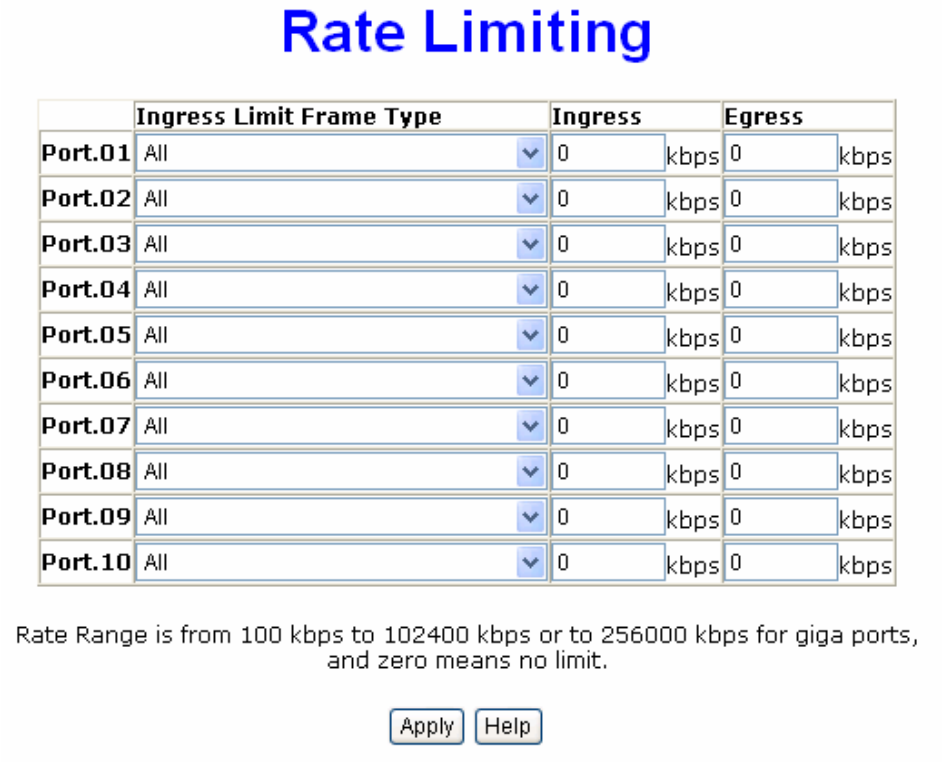


Port Trunk – Port Mirroring interface

Rate Limiting

You can set up every port's bandwidth rate and frame limitation type.

- **Ingress Limit Frame type:** select the frame type that you want to filter. The frame types have 4 options for selecting: **All, Broadcast/Multicast/Flooded Unicast, Broadcast/Multicast** and **Broadcast only**.
  Broadcast/Multicast/Flooded Unicast, Broadcast/Multicast and **Broadcast only** types are only for ingress frames. The egress rate only supports **All** types.


Rate Limiting
Ingress Limit Frame Type
Ingress
Egress
Port.01 All 0 kbps 0 kbps
Port.02 All 0 kbps 0 kbps
Port.03 All 0 kbps 0 kbps
Port.04 All 0 kbps 0 kbps
Port.05 All 0 kbps 0 kbps
Port.06 All 0 kbps 0 kbps
Port.07 All 0 kbps 0 kbps
Port.08 All 0 kbps 0 kbps
Port.09 All 0 kbps 0 kbps
Port.10 All 0 kbps 0 kbps
Rate Range is from 100 kbps to 102400 kbps or to 256000 kbps for giga ports, and zero means no limit.
Apply
Help

Rate Limiting interface

- All the ports support port ingress and egress rate control. For example, assume port 1 is 10Mbps, users can set it's effective egress rate is 1Mbps, ingress rate is 500Kbps. The switch performs the ingress rate by packet counter to meet the specified rate
  - **Ingress:** Enter the port effective ingress rate(The default value is "0")
  - **Egress:** Enter the port effective egress rate(The default value is "0")
- And then, click Apply to apply the settings

[NOTE] Rate Range is from 64 kbps to 102400 kbps (250000 kbps for giga ports) and zero means no limit

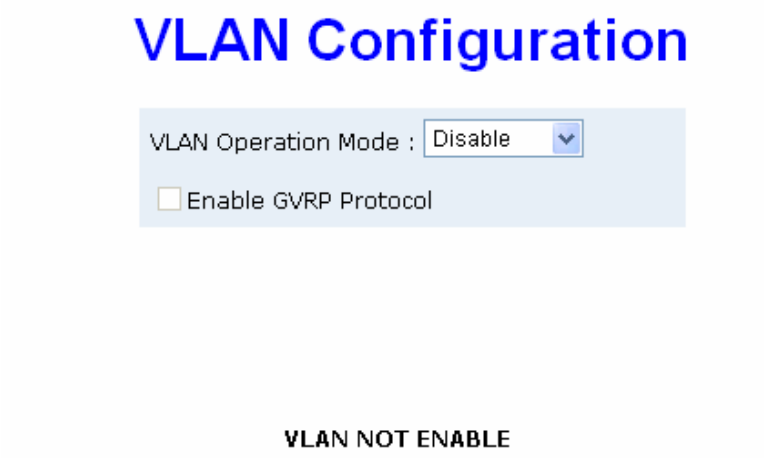
---

VLAN configuration

A Virtual LAN (VLAN) is a logical network grouping that limits the broadcast domain, which would, allow you to isolate network traffic so only the members of the VLAN will

receive traffic from the same members of VLAN. Basically, creating a VLAN from a switch is logically equivalent of reconnecting a group of network devices to another Layer 2 switch. However, all the network devices are still plugged into the same switch physically.

The industrial switch supports port-based and 802.1Q (tag-based) VLANs. In the default configuration, the VLAN operation mode default is "**Disable**".

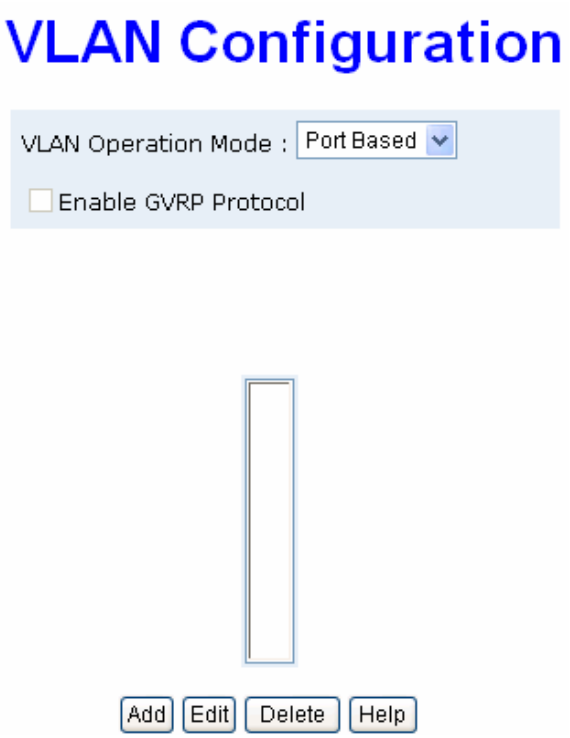


VLAN Configuration interface

VLAN configuration - Port-based VLAN

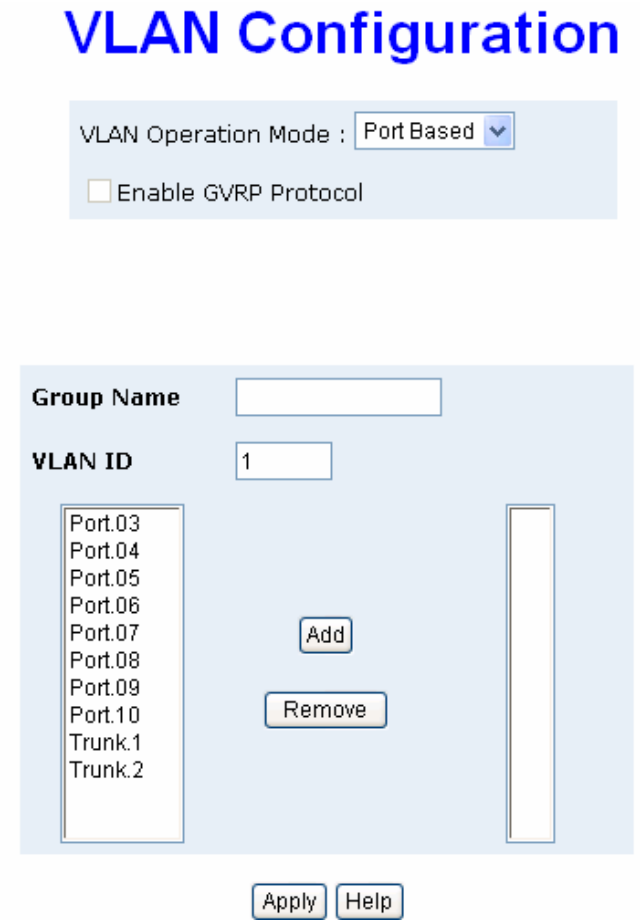
Packets can only go among members of the same VLAN group. Note all unselected ports are treated as belonging to another single VLAN. If the port-based VLAN is enabled, the VLAN-tagging is ignored.

In order for an end station to send packets to different VLAN groups, it has to be either capable of tagging the packets it sends with VLAN tags or attached to a VLAN-aware bridge that is capable of classifying and tagging the packet with a different VLAN ID based on not only default PVID but also other information about the packet, such as the protocol.



VLAN – Port Based interface

- Click Add to add a new VLAN group(The maximum VLAN group is up to 64 VLAN groups)
- Entering the VLAN name, group ID and grouping the members of VLAN group
- And then, click Apply



VLAN—Port Based Add interface

- You will see the VLAN displays.
- Use Delete button to delete unwanted VLAN.
- Use Edit button to modify existing VLAN group.

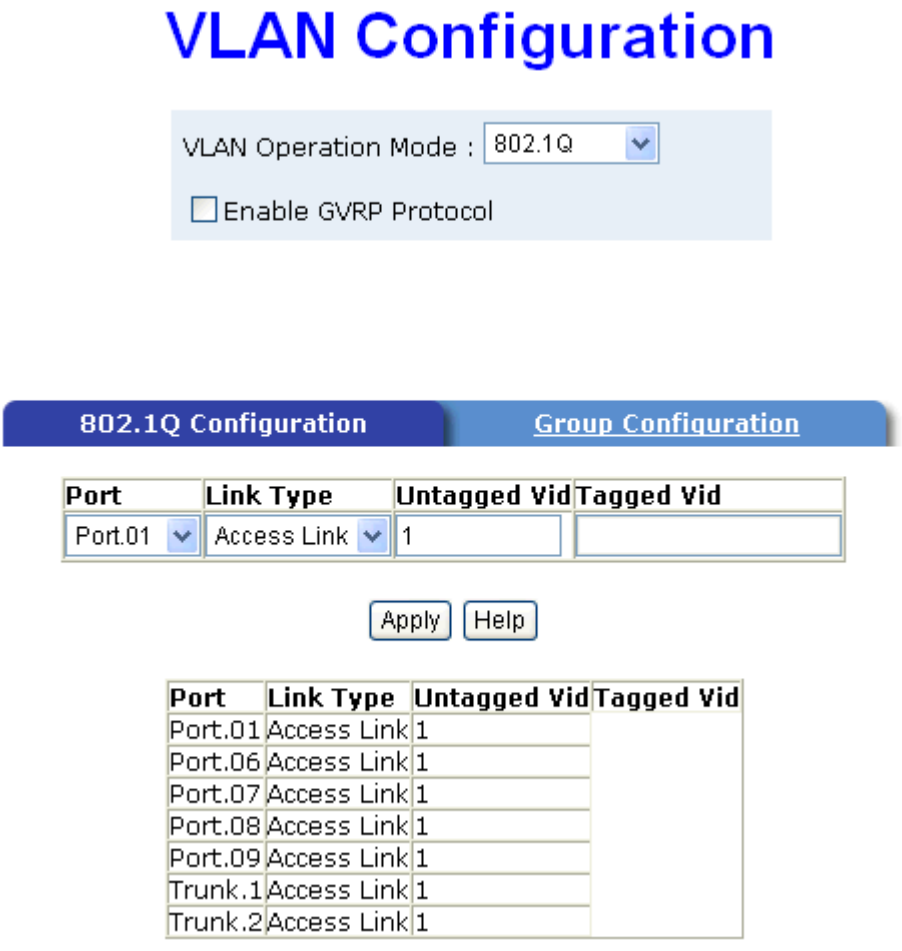
[NOTE] Remember to execute the “Save Configuration” action, otherwise the new configuration will be lost when switch is powered off.

802.1Q VLAN

A tag-based VLAN is an IEEE 802.1Q specification standard. Therefore, it is possible to create a VLAN across devices from different switch venders. IEEE 802.1Q VLAN uses a technique to insert a “tag” into the Ethernet frames. A tag contains a VLAN Identifier (VID) that indicates the VLAN numbers.

You can create a tag-based VLAN, and enable or disable GVRP protocol. There are 256 possible VLAN groups. To enable a 802.1Q VLAN, all the ports on the switch belong to the default VLAN, VID is 1. The default VLAN can’t be deleted.

GVRP allows automatic VLAN configuration between the a switch and its nodes. If the switch is connected to a device with GVRP enabled, you can send a GVRP request using the VID of a VLAN defined on the switch; the switch will automatically add that device to the existing VLAN.



802.1q VLAN interface

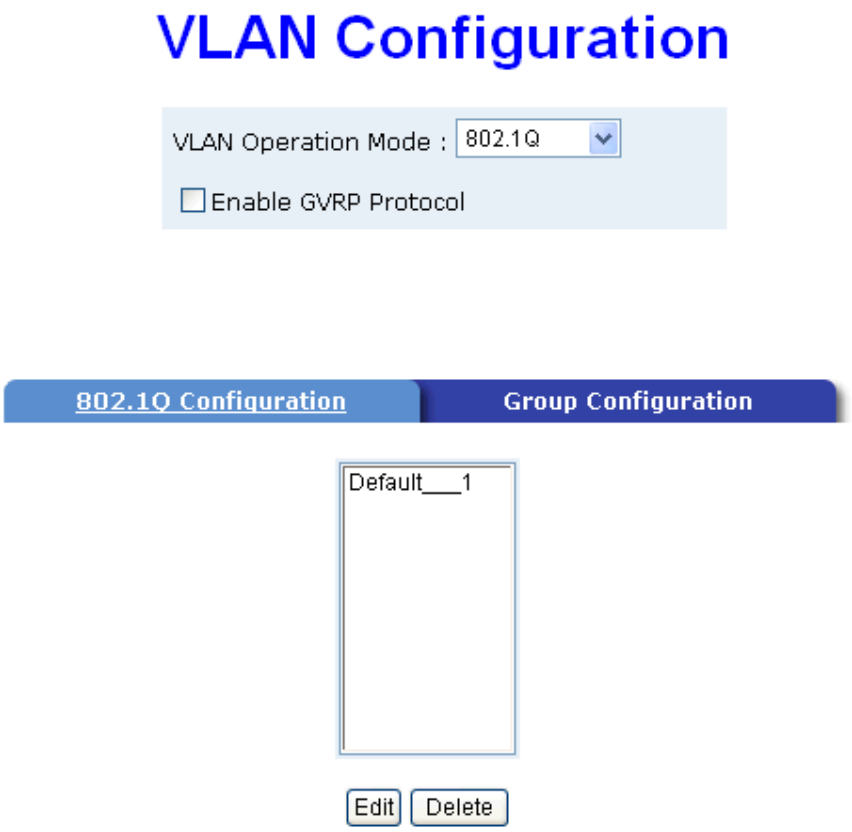
802.1Q Configuration

1. **Enable GVRP Protocol:** check the check box to enable GVRP protocol.
2. Select the port that you want to configure.
3. **Link Type**: there are 3 types of link type.
   - **Access Link:** single switch only, allow user to group ports by setting the same VID.
   - **Trunk Link:** extended application of **Access Link**, allow user to group ports by setting the same VID with 2 or more switches.
   - **Hybrid Link:** Both **Access Link** and **Trunk Link** are available.
4. **Untagged VID:** assign the untagged frame VID.
5. **Tagged VID:** assign the tagged frame VID.
6. Click Apply
7. You can see each port setting in the below table on the screen.

Group Configuration

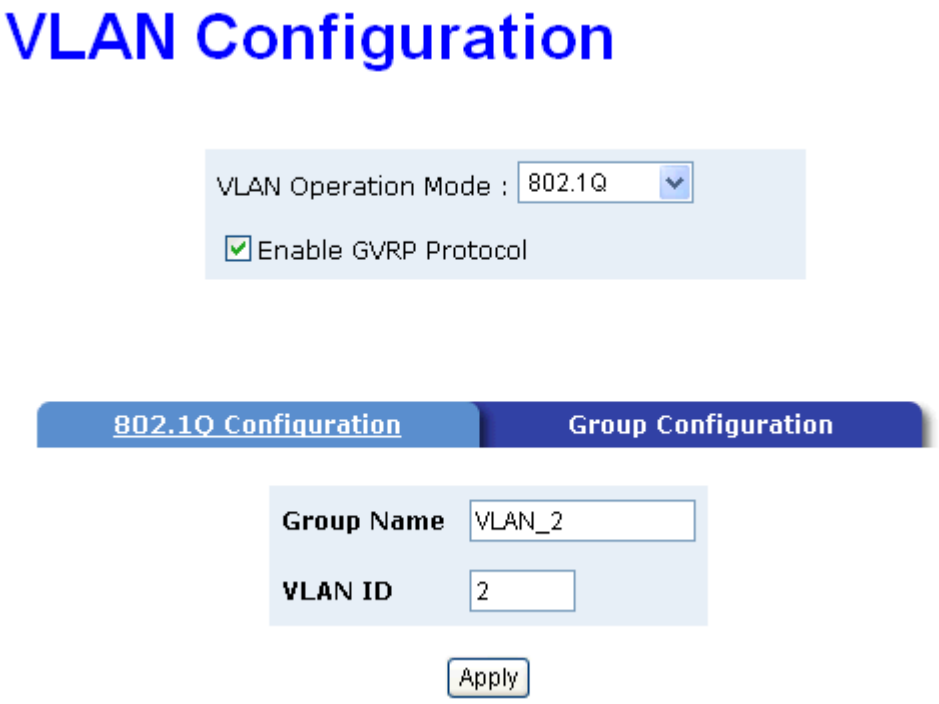
Edit the existing VLAN Group.

1. Select the VLAN group in the table list.
2. Click Apply



Group Configuration interface

3. You can change the VLAN group name and VLAN ID.
4. Click Apply.



Group Configuration interface

Rapid Spanning Tree

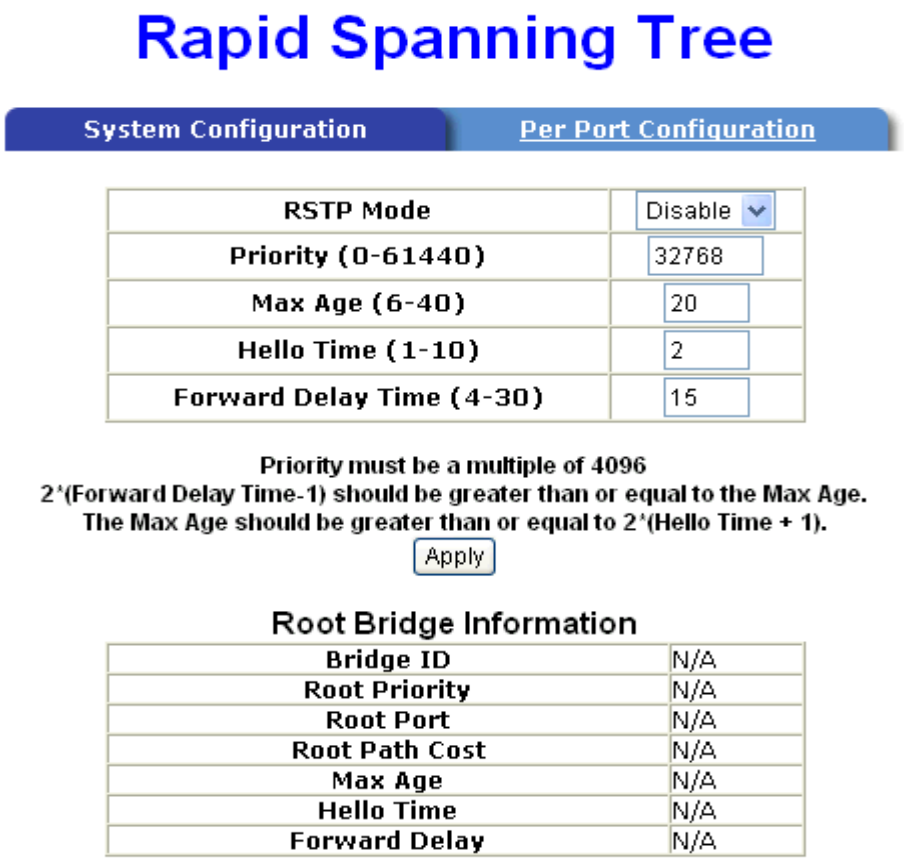
The Rapid Spanning Tree Protocol (RSTP) is an evolution of the Spanning Tree Protocol and provides for faster spanning tree convergence after a topology change. The system also supports STP and the system will auto detect the connected device that is running STP or RSTP protocol.

RSTP System Configuration

- User can view spanning tree information about the Root Bridge
- User can modify RSTP state. After modification, click Apply button
  - **RSTP mode:** the user must enable or disable RSTP function before configuring the related parameters
  - **Priority (0-61440):** a value used to identify the root bridge. The bridge with the lowest value has the highest priority and is selected as the root. If the value changes, the user must reboot the switch. The value must be multiple of 4096 according to the protocol standard rule
  - **Max Age (6-40):** the number of seconds a bridge waits before receiving Spanning-tree Protocol configuration messages before attempting a reconfiguration. Enter a value between 6 through 40
  - **Hello Time (1-10):** the number of seconds before the control switch sends out the BPDU packet to check RSTP current status. Enter a value between 1 through 10
  - **Forward Delay Time (4-30):** the number of seconds a port waits before changing from its Rapid Spanning-Tree Protocol learning and listening states to the forwarding state. Enter a value between 4 through 30

[NOTE] Follow the rule to configure the MAX Age, Hello Time, and Forward Delay Time.

2 x (Forward Delay Time value –1) > = Max Age value >= 2 x (Hello Time value +1)



RSTP System Configuration interface

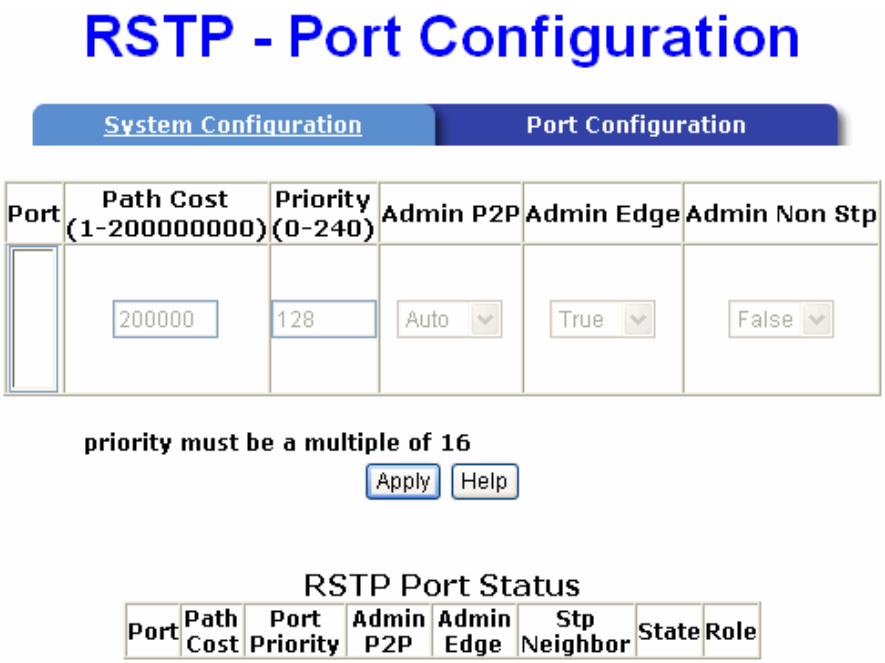
RSTP Per Port Configuration

You can configure the path cost and priority of every port.

1. Select the port in Port column.
1. **Path Cost:** The cost of the path to the other bridge from this transmitting bridge at the specified port. Enter a number 1 through 200000000.
2. **Priority:** Decide which port should be blocked by priority in the LAN. Enter a number 0 through 240. The value of the priority must be a multiple of 16.
3. **P2P:** Some of the rapid state transactions that are possible within RSTP are dependent upon whether the port concerned can only be connected to exactly one other bridge (i.e. it is served by a point-to-point LAN segment), or can be connected to two or more bridges (i.e. it is served by a shared medium LAN segment). This function allows the P2P status of the link to be manipulated administratively. True is P2P enabling. False is P2P disabling.
4. **Edge:** The port directly connected to end stations cannot create a bridging loop in

the network. To configure the port as an edge port, set the port to "**True**" status.

5. **Non Stp:** The port includes the STP mathematic calculation. **True** does not include the STP mathematic calculation. **False** is included in the STP mathematic calculation.
6. Click Apply.



RSTP Per Port Configuration interface

SNMP Configuration

Simple Network Management Protocol (SNMP) is the protocol developed to manage nodes (servers, workstations, routers, switches and hubs etc.) on an IP network. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth. Network management systems learn of problems by receiving traps or change notices from network devices implementing SNMP.

System Configuration

- **Community Strings**

You can define a new community string set and remove an unwanted community string.

1. **String:** fill the name of string.
2. **RO:** Read only. Enables requests accompanied by this string to display MIB-object information.
3. **RW:** Read write. Enables requests accompanied by this string to display MIB-object information and to set MIB objects.

1. Click Add.
2. To remove the community string, select the community string that you have defined and click Remove. You cannot remove the default community string set.

- **Agent Mode:** Select the SNMP version that you want to use it. And then click Change to switch to the selected SNMP version mode.

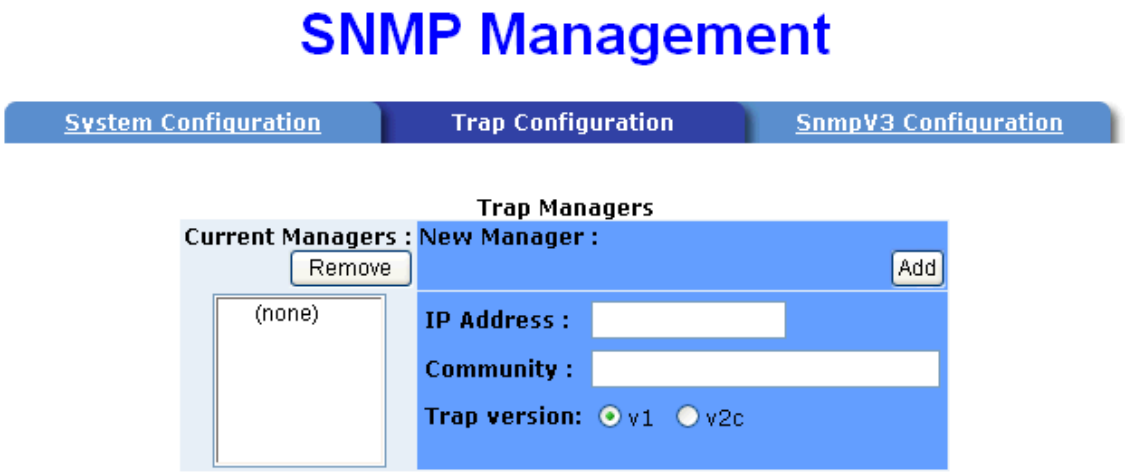
SNMP System Configuration interface

Trap Configuration

A trap manager is a management station that receives traps and system alerts

generated by the switch. If no trap manager is defined, no traps will be issued. Create a trap manager by entering the IP address of the station and a community string. To define management stations as trap managers and to enter SNMP community strings and selects the SNMP version.

1. **IP Address:** enter the IP address of trap manager.
2. **Community:** enter the community string.
3. **Trap Version:** select the SNMP trap version type – v1 or v2.
4. Click Add.
5. To remove the community string, select the community string that you have defined and click Remove. You cannot remove the default community string set.



Trap Managers interface

SNMPV3 Configuration

Configure the SNMP V3 function.

Context Table

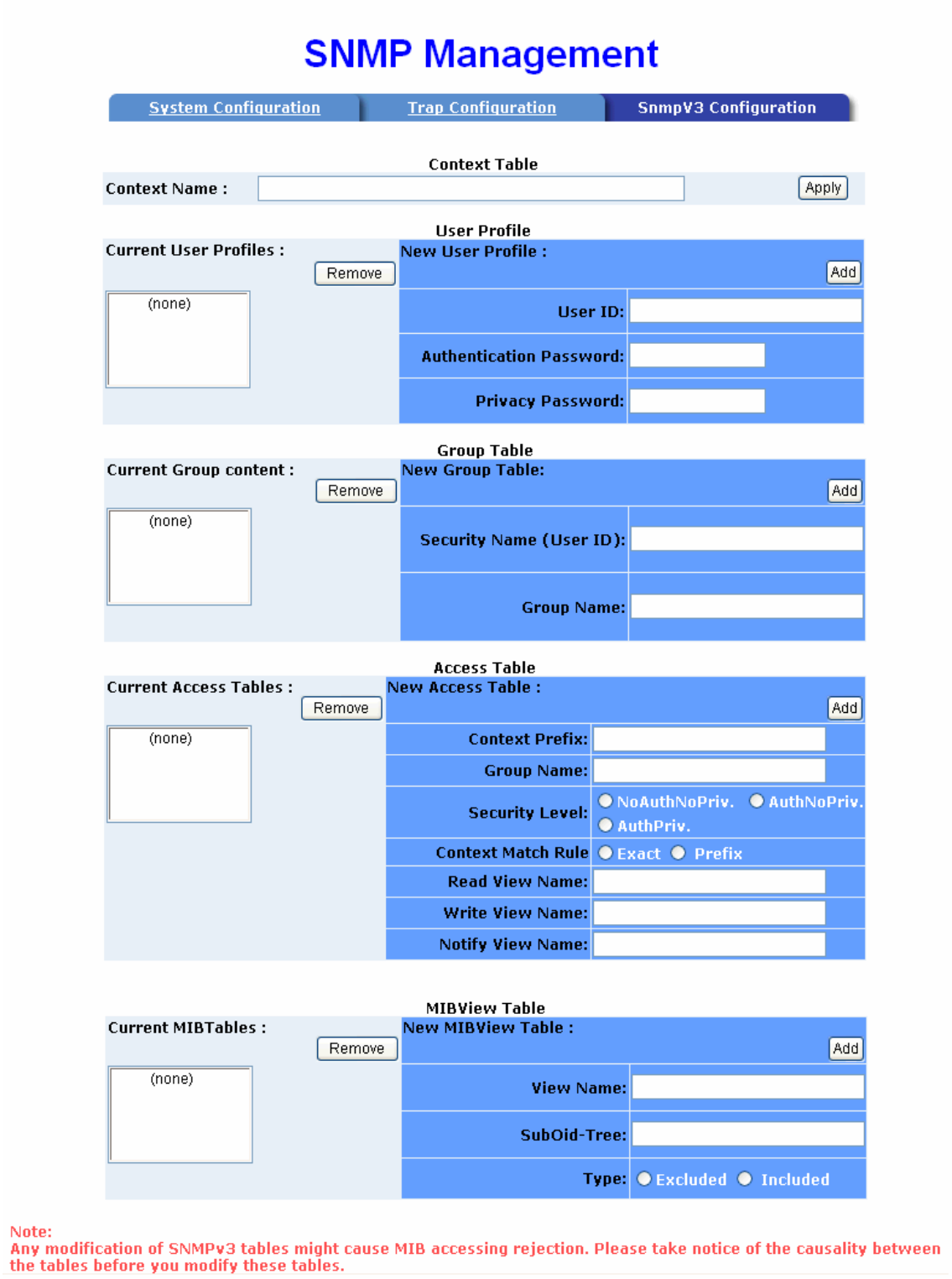
Configure SNMP v3 the context table. Assign the context name of the context table. Click Add to add context name. Click Remove to remove unwanted context name.

User Profile

Configure the SNMP v3 user table..

- **User ID:** set up the user name.
- **Authentication Password:** set up the authentication password.
- **Privacy Password:** set up the private password.
- Click Add to add context name.

Click Remove to remove unwanted context name.



SNMP V3 configuration interface

Group Table

Configure the SNMP v3 group table.

- **Security Name (User ID):** assign the user name that you have set up in user table.
- **Group Name:** set up the group name.

- Click Add to add context name.
- Click Remove to remove unwanted context name.

Access Table

Configure the SNMP v3 access table.

- **Context Prefix:** set up the context name.
- **Group Name:** set up the group.
- **Security Level:** select the access level.
- **Context Match Rule:** select the context match rule.
- **Read View Name:** set up the read view.
- **Write View Name:** set up the write view.
- **Notify View Name:** set up the notify view.
- Click Add to add context name.
- Click Remove to remove unwanted context name.

MIBview Table

Configure the MIB view table.

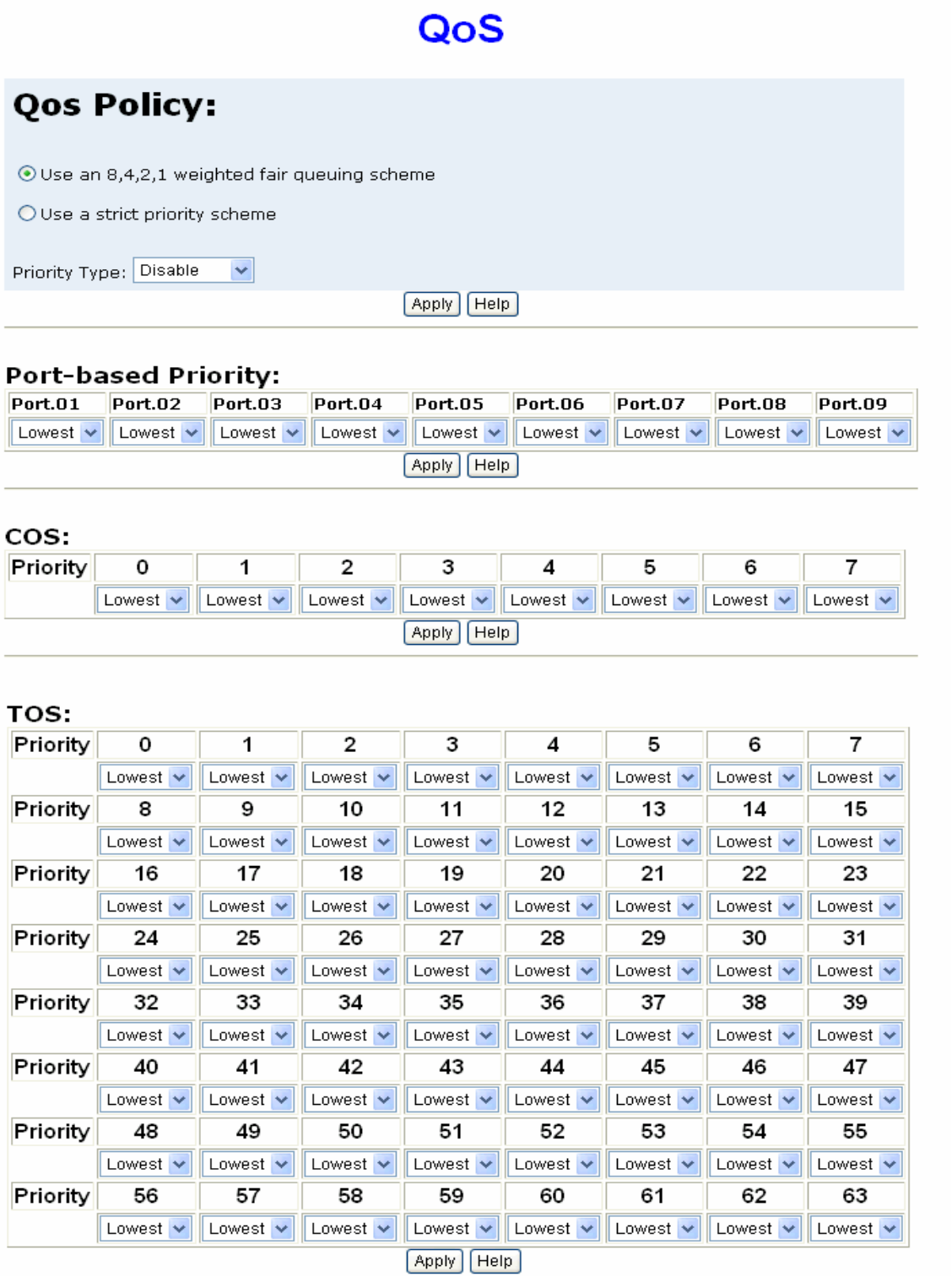
- **ViewName:** set up the name.
- **Sub-Oid Tree:** fill the Sub OID.
- **Type:** select the type – exclude or included.
- Click Add to add context name.
- Click Remove to remove unwanted context name.

QoS Configuration

You can configure QoS policy and priority setting, per port priority setting, COS and TOS setting.

QoS Policy and Priority Type

- **QoS Policy:** select the QoS policy rule.
  - **Using the 8,4,2,1 weight fair queue scheme:** The switch will follow a 8:4:2:1 rate to process priority queue from the Highest to the lowest queue. For example: the system will process 80 % high queue traffic, 40 % middle queue traffic, 20 % low queue traffic, and 10 % lowest queue traffic at the same time. The traffic in the Low Priority queue is not transmitted until all High, Medium, and Normal traffic are serviced.
  - **Use the strict priority scheme:** The higher queues will be process first, except if the higher queues are empty.
- **Priority Type:** there are 5 priority type selections available. Disable means that no priority type is selected.
- **Port-base:** the port priority will follow the **Port-base** that you have assigned – High, middle, low, or lowest.
  - **COS only:** the port priority will only follow the **COS priority** that you have assigned.
  - **TOS only:** the port priority will only follow the **TOS priority** that you have assigned.
  - **COS first:** the port priority will follow the COS priority first, and then other priority rule.
  - **TOS first:** the port priority will follow the TOS priority first, and the other priority rule.
- Click Apply.


QoS
Qos Policy:
Use an 8,4,2,1 weighted fair queuing scheme
Use a strict priority scheme
Priority Type: Disable
Apply Help
Port-based Priority:
Port.01 Port.02 Port.03 Port.04 Port.05 Port.06 Port.07 Port.08 Port.09
Lowest
Apply Help
COS:
Priority 0 1 2 3 4 5 6 7
Lowest
Apply Help
TOS:
Priority 0 1 2 3 4 5 6 7
Priority 8 9 10 11 12 13 14 15
Priority 16 17 18 19 20 21 22 23
Priority 24 25 26 27 28 29 30 31
Priority 32 33 34 35 36 37 38 39
Priority 40 41 42 43 44 45 46 47
Priority 48 49 50 51 52 53 54 55
Priority 56 57 58 59 60 61 62 63
Lowest
Apply Help

QoS Configuration interface

Port Base Priority

Configure port priority level.

- **Port 1 ~ Port 10:** each port has 4 priority levels – High, Middle, Low, and Lowest.

- Click Apply.

COS Configuration

Set up the COS priority level.

- **COS priority:** Set up the COS priority level 0~7 –High, Middle, Low, Lowest.
- Click Apply.

TOS Configuration

Set up the TOS priority.

- **TOS priority:** the system provides 0~63 TOS priority level. Each level has 4 types of priority – high, middle, low, and lowest. The default value is “Lowest” priority for each level. When the IP packet is received, the system will check the TOS level value in the IP packet that it has received. For example: the user sets the TOS to level 25 - high. The port is following the TOS priority policy only. When the port 1 packet is received, the system will check the TOS value of the received IP packet. If the TOS value of received IP packet is 25(priority = high), then the packet will have highest priority.
- Click Apply.

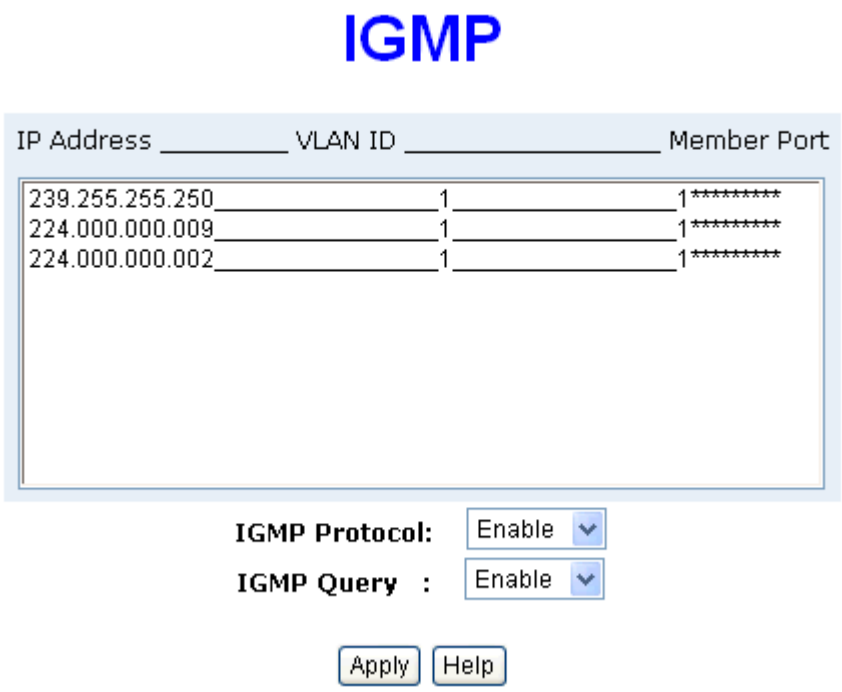
IGMP Configuration

The Internet Group Management Protocol (IGMP) is an internal protocol of the Internet Protocol (IP) suite. IP manages multicast traffic by using switches, routers, and hosts that support IGMP. Enabling IGMP allows the ports to detect IGMP queries and report packets and manage IP multicast traffic through the switch. IGMP has three fundamental types of messages as follows:

Message	Description
Query	A message sent from the querier (IGMP router or switch) asking for a response from each host belonging to the multicast group.
Report	A message sent by a host to the querier to indicate that the host wants to be or is a member of a given group indicated in the report message.
Leave Group	A message sent by a host to the querier to indicate that the host has quit being a member of a specific multicast group.

If the switch supports IP multicasting, you can enable the IGMP protocol on the switch's management setting advanced page, then display the IGMP snooping information. IP multicast addresses range from 224.0.0.0 through 239.255.255.255.

- **IGMP Protocol:** enable or disable the IGMP protocol.
- **IGMP Query:** enable or disable the IGMP query function. The IGMP query information will be display in IGMP status section.
- Click Apply.



X-Ring

The X-Ring provides a faster redundant recovery than Spanning Tree topology. The action is similar to STP or RSTP, but the algorithms are not the same.

In the X-Ring topology, every switch should have X-Ring function enabled and two member ports assigned for the ring. Only one switch in the X-Ring group would be set as the Redundancy Manager (RM) – the switch that has two ports, one, called the backup port, and the other port is called the working port. Other switches are called working switches and their two member ports are called working ports. When the failure of a network connection occurs, the backup port will automatically become a working port to recover from the failure and allow network traffic to continue.

The RM can negotiate and place commands to other switches in the X-Ring group. If there are 2 or more switches in RM mode, then the software will select the switch with lowest MAC address number as the RM. The X-Ring RM mode will be enabled by the X-Ring configuration interface. Also, user can identify the switch as the RM from the R.M. LED panel of the LED panel on the switch.

The system also supports the coupling ring that can connect 2 or more X-Ring groups for the redundant backup function and dual homing function that prevent connection loss between X-Ring group and upper level/core switches.

- **Enable X-Ring:** To enable the X-Ring function. Mark the check box to enable the X-Ring function.
- **Enable Ring Master:** Mark the check box for enabling this switch to be the ring Redundancy Manager (RM)
- **1st & 2nd Ring Ports:** Pull down the selection menu to assign two ports as the member ports. **1st Ring Port** is the working port and **2nd Ring Port** is the backup port. If the **1st Ring Port** fails, the system will automatically upgrade the **2nd Ring Port** to be the working port.
- **Enable Coupling Ring:** To enable the coupling ring function. Marking the check box to enable the coupling ring function.

- **Coupling port:** Assign the member port.
- **Control port:** Set the switch as the master switch in the coupling ring.
- **Enable Dual Homing:** Set up one of port on the switch to be the Dual Homing port. In an X-Ring group, maximum Dual Homing ports is one. Dual Homing only works when the X-Ring function is enabled.
- And then, click Apply to apply the configuration.

X-ring Interface

[NOTE]

1. When the X-Ring function is enabled, the user must disable RSTP. The X-Ring function and RSTP function cannot exist at the same time.
2. Remember to execute the “Save Configuration” action, otherwise the new configuration will be lost when switch is powered off.

Security

In this section, you can configure 802.1x and MAC address table.

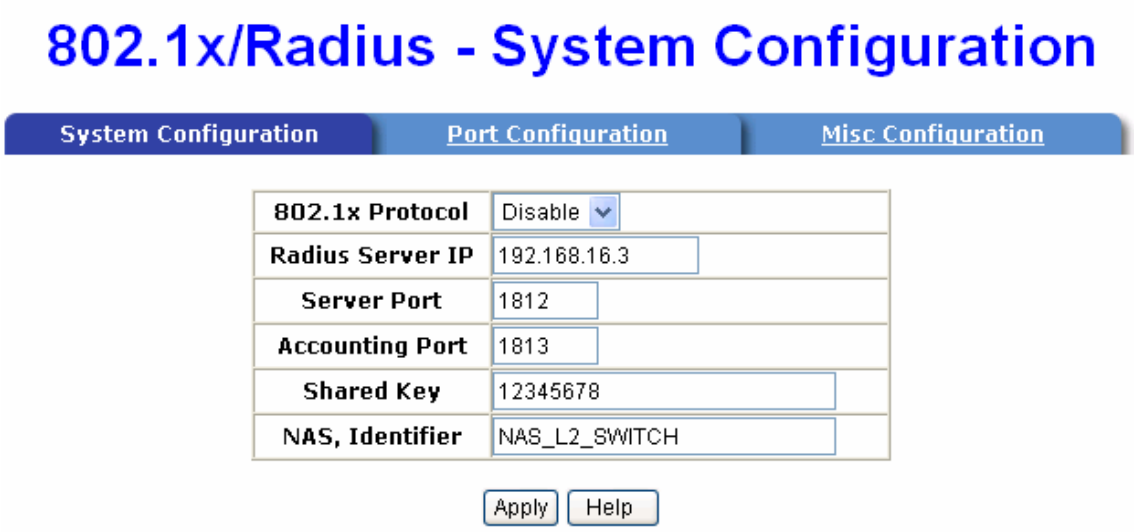
802.1X/Radius Configuration

802.1x is an IEEE authentication specification that allows a client to connect to a wireless access point or wired switch but prevents the client from gaining access to the Internet until it provides authority, like a user name and password that are verified by a separate server.

System Configuration

After enabling the IEEE 802.1X function, you can configure the parameters of this function.

1. **IEEE 802.1x Protocol:** .enable or disable 802.1x protocol.
2. **Radius Server IP:** set the Radius Server IP address.
3. **Server Port:** set the UDP destination port for authentication requests to the specified Radius Server.
4. **Accounting Port:** set the UDP destination port for accounting requests to the specified Radius Server.
5. **Shared Key:** set an encryption key for using during authentication sessions with the specified radius server. This key must match the encryption key used on the Radius Server.
6. **NAS, Identifier:** set the identifier for the radius client.
7. Click Apply.

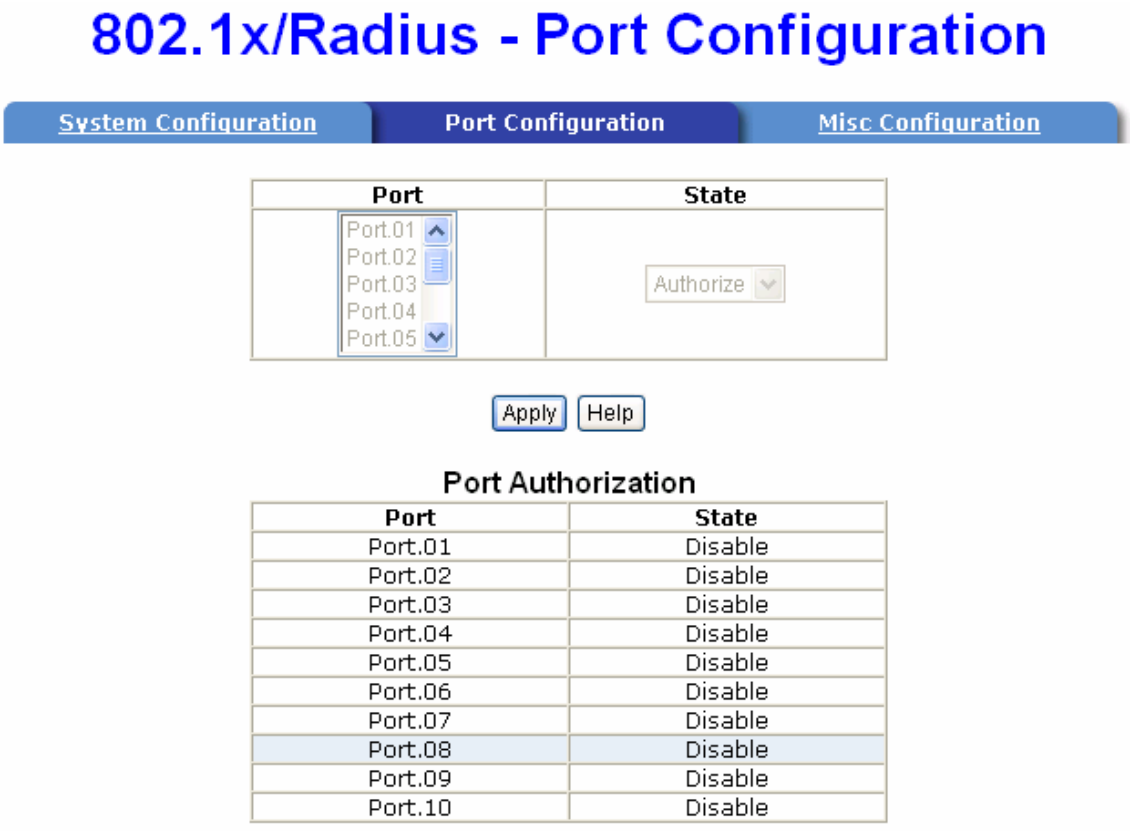


802.1x System Configuration interface

802.1x Per Port Configuration

You can configure the 802.1x authentication state for each port. The State provides Disable, Accept, Reject and Authorize. Use "**Space**" key change the state value.

- **Reject:** the specified port is required to be held in the unauthorized state.
- **Accept:** the specified port is required to be held in the Authorized state.
- **Authorized:** the specified port is set to the Authorized or Unauthorized state in accordance with the outcome of an authentication exchange between the Supplicant and the authentication server.
- **Disable:** The specified port is required to be held in the Authorized state
- Click Apply.

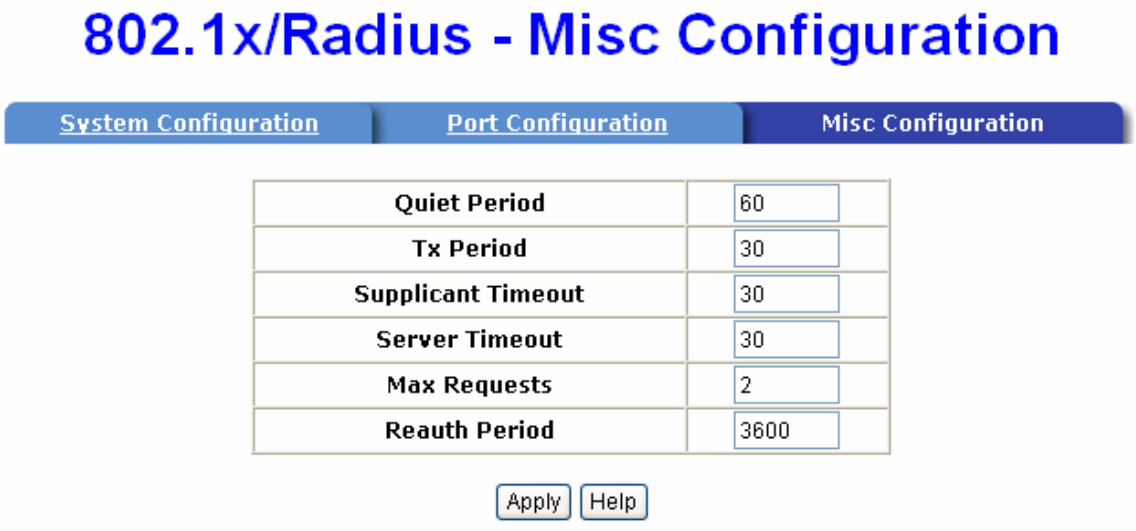


802.1x Per Port Setting interface

Misc. Configuration

1. **Quiet Period:** set the period during which the port doesn't try to acquire a supplicant.

2. **TX Period:** set the period the port wait for retransmit next EAPOL PDU during an authentication session.
3. **Supplicant Timeout:** set the period of time the switch waits for a supplicant response to an EAP request.
4. **Server Timeout:** set the period of time the switch waits for a server response to an authentication request.
5. **Max Requests:** set the number of authentication that must time-out before authentication fails and the authentication session ends.
6. **Reauth period:** set the period of time after which clients connected must be re-authenticated.
7. Click Apply.



802.1x Misc Configuration interface

MAC Address Table

Use the MAC address table to ensure the port security.

Static MAC Address

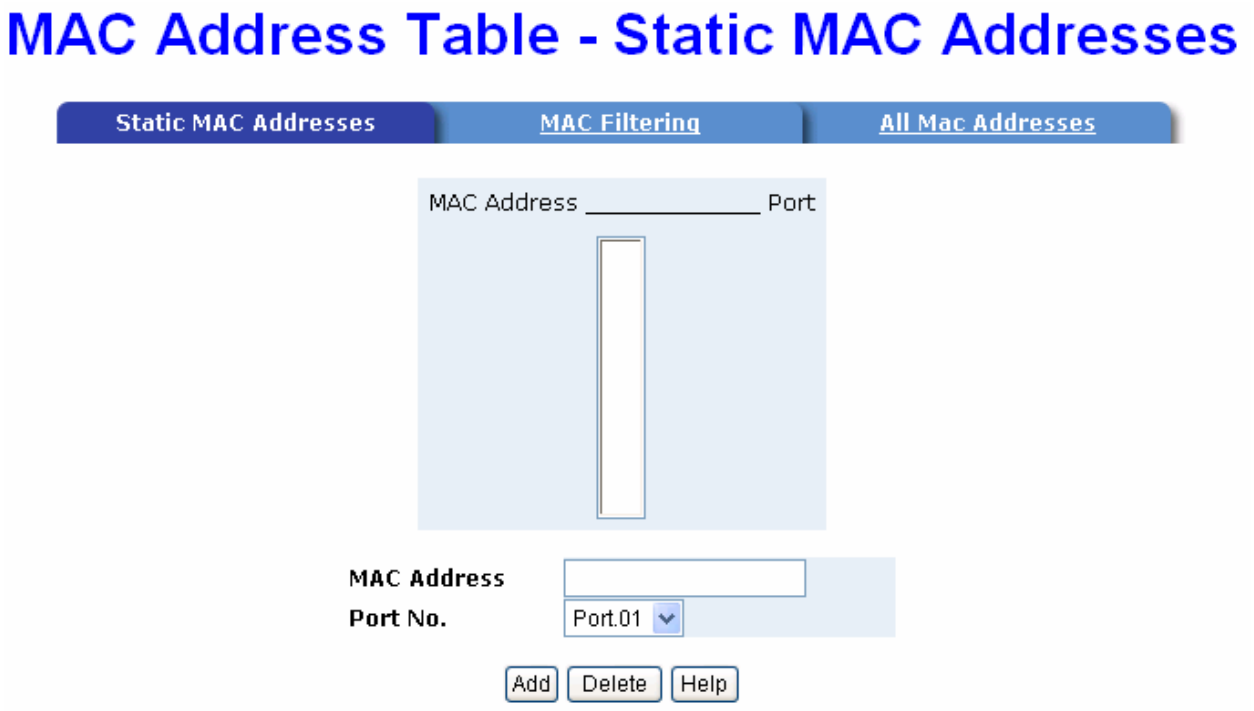
You can add a static MAC address; it remains in the switch's address table, regardless of whether the device is physically connected to the switch. This saves the switch from

having to re-learn a device's MAC address when the disconnected or powered-off device is active on the network again. You can add / modify / delete a static MAC address.

■ **Add the Static MAC Address**

You can add static MAC address in switch MAC table.

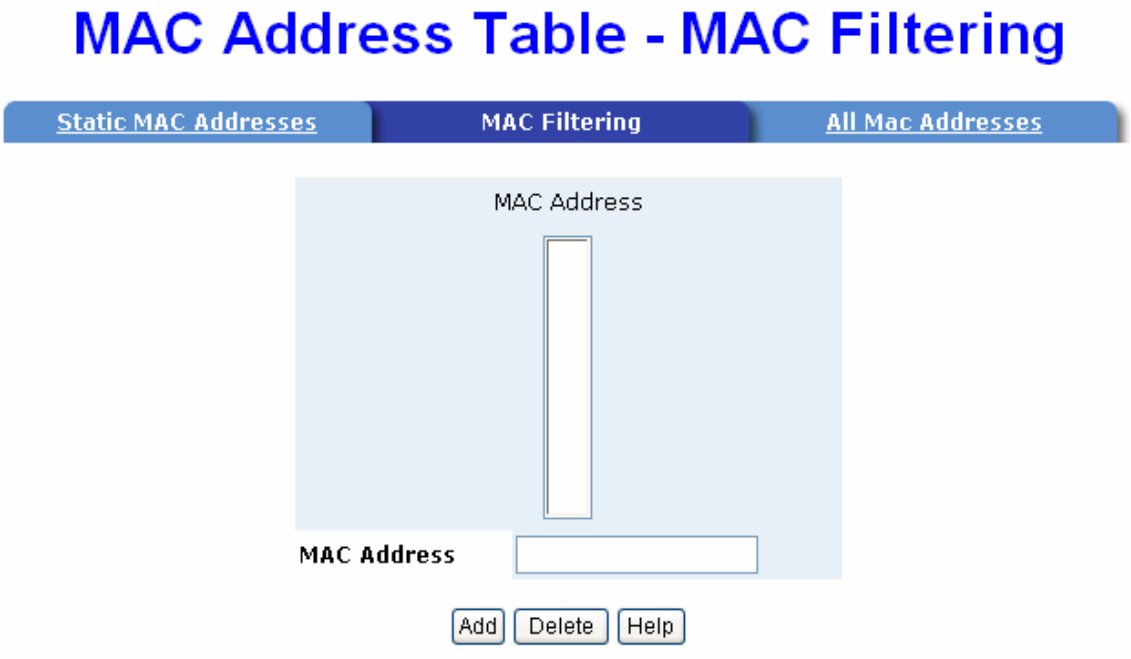
1. **MAC Address:** Enter the MAC address of the port that should permanently forward traffic, regardless of the device network activity.
2. **Port No.:** pull down the selection menu to select the port number.
3. Click Add .
4. If you want to delete the MAC address from filtering table, select the MAC address and click Delete .



Static MAC Addresses interface

MAC Filtering

By filtering the MAC address, the switch can easily filter pre-configured MAC addresses and enhance security . You can add and delete filtering MAC addresses.



MAC Filtering interface

1. **MAC Address:** Enter the MAC address that you want to filter.
2. Click Add.
3. If you want to delete the MAC address from filtering table, select the MAC address and click Delete.

All MAC Addresses

You can view the port that connected device's MAC address and related devices' MAC address.

1. Select the port.
2. The selected port of static MAC address information will display.
3. Click Clear MAC Table to clear the current port static MAC address information on screen.

All MAC Address interface

Factory Default

Reset the switch to a default configuration. Click Default to reset all configurations to the default value.

Factory Default interface

Save Configuration

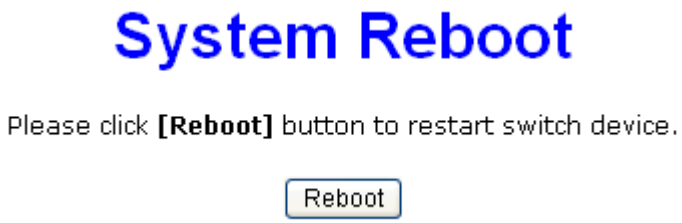
Save all configurations that you have made in the system. To ensure the all configurations will be saved. Click Save Flash to save the configuration to the flash

memory.

Save Configuration interface

System Reboot

Reboot the switch - a software reset. Click Reboot to reboot the system.



System Reboot interface

Troubleshooting

- Verify the right power cord/adapter (DC 24-48V), DO NOT use the power adapter with a DC output larger than 48V, or it will cause damage to the switch.
- Select the proper UTP cable to construct the network. Please check that is the correct cable type – CAT 5, etc. Use unshielded twisted-pair (UTP) or shielded twisted-pair (STP) cable for RJ-45 connections: 100Ω Category 3, 4 or 5 cable for 10Mbps connections or 100Ω Category 5 cable for 100Mbps connections. Also be sure that the length of any twisted-pair connection does not exceed 100 meters (328

feet).

- **Diagnostic LED Indicators:** the Switch can be easily monitored through panel indicators to assist in identifying problems, which describes common problems the user may encounter.
- If the power indicator does not turn on when the power is applied, the user may have a problem with the power supply. Check for loose power connections, power losses or surges at the power supply. If the user still cannot resolve the problem, contact user local dealer for assistance.
- If the Industrial switch LED indicators are normal and the connected cables are correct but the packets still do not transmit, check the user system's other devices on the network – duplicate IP addresses, etc. - other devices' configurations or status.

Technical Specifications

The 8 10/100TX plus 2 1000LX/SX managed industrial switch technical specification is following.

Standard	IEEE 802.3 10Base-T Ethernet IEEE 802.3u 100Base-TX and 100Base-FX Fast Ethernet IEEE802.3x Flow Control and Back-pressure IEEE802.1d spanning tree / IEEE802.1w rapid spanning tree IEEE802.1p class of service IEEE802.1Q VLAN Tag
Protocol	CSMA/CD
Management	SNMP management Web interface management One default button for system default setting
RFC Standard	RFC2030 SNTP RFC 2821 SMTP RFC 1215 Trap RFC2233 MIBII RFC 1157 SNMP MIB RFC 1493 Bridge MIB RFC 2674 VLAN MIB RFC 2665 Ethernet like MIB RFC 2819 RMON MIB Private MIB

SNMP Trap	Up to 3 Trap stations Cold start Port link Up Port link down Authentication Failure Private Trap for power status Port Alarm configuration Fault alarm, X-Ring
Technology	Store and forward switching architecture
Transfer Rate	14,880 pps for 10Base-T Ethernet port 148,800 pps for 100Base-TX/FX Fast Ethernet port 1,488,000 pps for Gigabit Fiber Ethernet port
Transfer packet size	64bytes to 1522 bytes (with VLAN tag)
Packet filter	4 types of packet filter rule with different packet combination: ■ All of packet ■ Broadcast/ multicast/ flooded unicast packet ■ Broadcast/ multicast packet ■ Broadcast packet only
MAC address	8K MAC address table
Memory Buffer	1Mbits
LED	**Per port:** Link/Activity (Green), Full duplex/Collision (Orange) **Per unit:** Power (Green), Power 1 (Green), Power 2 (Green), Fault (Orange), Master (Green)

Network Cable	10Base-T: 2-pair UTP/STP Cat. 3, 4, 5 cable EIA/TIA-568 100-ohm (100m) 100Base-TX: 2-pair UTP/STP Cat. 5 cable EIA/TIA-568 100-ohm (100m)
Optical cable	■ **SC (Multi-mode):** 50/125um or 62.5/125um ■ **SC (Single mode):** 9/125um or 10/125um ■ **Available distance:** 2KM (Multi-mode) / 30KM (single-mode) ■ **Wavelength:** 1310nm (multi-mode/ single mode)
Back-plane	5.6Gbps
Packet throughput ability	8.3Mpps at 64bytes
Power Supply	24 ~48 VDC Redundant power with polarity reverse protects function and connective removable terminal block for master and slave power.
Power consumption	9.2 Watts
X-Ring	2 ports for X-Ring to provide redundant backup feature and the recovery time below 300ms and configured by Web interface management. The ring port can be defined by Web interface.
VLAN	Port based VLAN IEEE802.1Q Tag VLAN. Port based and Tag based VLAN groups up to 256 VLANs.

Class of service	IEEE802.1p class of service Per port provides 4 priority queues.
Quality of service	Port based/Tag based, IPv4 ToS, IPv6 Different Service.
Spanning tree	IEEE802.1d spanning tree IEEE802.1w rapid spanning tree.
IGMP	IGMP v1, v2 and Query mode Up to 256 multicast groups.
SMTP	Simple mail transfer protocol.
SNTP	Simple Network time protocol.
Management IP security	IP address security to prevents unauthorized intruder
Port mirror	TX packet only RX packet only, Both of TX and RX packet
Firmware update	TFTP firmware update TFTP backup and restore
Alarm	One relay output for port breakdown and power fail alarm Alarm Relay current carry ability: 1A @ DC24V

Bandwidth control	■ Ingress packets filter and egress packet limit. ■ The egress rate control supports all of packet type and the limit rate range is from 100 kbps to 102400 kbps or to 256000 kbps for giga ports, and zero means no limit. ■ Ingress filter packet type combination rule for Broadcast/Multicast/Flooded Unicast packet, Broadcast/Multicast packet, Broadcast packet only and all of packet. ■ The ingress packet filter rate range is from 100 kbps to 102400 kbps or to 256000 kbps for giga ports, and zero means no limit.
DHCP client	DHCP client function to obtain IP address from DHCP serve
Install	DIN rail kit and wall mount ear for wall mount or DIN-type cabinet install
Operation Temp.	-10℃ to 70℃
Operation Humidity	5% to 95% (Non-condensing)
Storage Temperature	-40℃ to 85℃
Case Dimension	IP-30, 72 mm (W) x 105 mm (D) x 152mm (H)
EMI	FCC Class A CE EN6100-4-2 CE EN6100-4-3 CE EN-6100-4-4 CE EN6100-4-5 CE EN6100-4-6

Safety	UL cUL CE/EN60950
Stability testing	IEC60068-2-32 (Free fall) IEC60068-2-27 (Shock) IEC60068-2-6 (Vibration)